



**Calhoun: The NPS Institutional Archive**  
**DSpace Repository**

---

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

---

2009-03

Exploring the lack of interoperability of databases within Department of Homeland Security interagency environment concerning maritime port security

Olk, Jeffrey S.

Monterey, California. Naval Postgraduate School

---

<http://hdl.handle.net/10945/4807>

---

*Downloaded from NPS Archive: Calhoun*



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

<http://www.nps.edu/library>



**NAVAL  
POSTGRADUATE  
SCHOOL  
MONTEREY, CALIFORNIA**

**THESIS**

**EXPLORING THE LACK OF INTEROPERABILITY OF DATABASES  
WITHIN DEPARTMENT OF HOMELAND SECURITY INTERAGENCY  
ENVIRONMENT CONCERNING MARITIME PORT SECURITY**

by

Jeffrey S. Olk

March 2009

Thesis Advisor:  
Second Reader:

Alex Bordetsky  
Michael Clement

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Exploring the Lack of Interoperability of Databases within Department of Homeland Security Interagency Environment Concerning Maritime Port Security.		5. FUNDING NUMBERS	
6. AUTHOR: Jeffrey Olk			
7. PERFORMING ORGANIZATION NAME (S) AND ADDRESS (ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME (S) AND ADDRESS(ES) N/A		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) Federal agencies that are within The Department of Homeland Security have many missions to support the security of the United States. One mission concurrent with this thesis topic is Maritime Interdiction Operations, which protects America's maritime borders from all intrusions by halting the flow of illegal drugs, aliens, and contraband into the United States through maritime routes. All government agencies within The Department of Homeland Security are continuing to focus their effort in sharing critical data to improve their situational awareness (SA) of command and control (C2), to make quicker decisions, and to collaborate with remote experts in support of another possible terrorist attack. Unfortunately this effort is being accomplished without the foresight of interoperability of existing databases throughout the interagency within The Department of Homeland Security. The lack of interoperability of these databases between the interagency continues to be a major issue in the security and safety to our nation's maritime ports. This thesis will discuss the lack of interoperability of databases between federal, state and local law enforcement agencies. The need and urgency to collaborate these vital databases into one unified decentralized network-to store and retrieve critical information to protect our maritime ports of entry, when needed, to protect our nation from any possible future threats that may harm our nation-is also stressed.			
14. SUBJECT TERMS: Interoperability, HSIN, Department of Homeland Security, Command and Control, Situational Awareness, Maritime Port Security, USCG, CBP.			15. NUMBER OF PAGES 89
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXPLORING THE LACK OF INTEROPERABILITY OF DATABASES WITHIN  
DEPARTMENT OF HOMELAND SECURITY INTERAGENCY ENVIRONMENT  
CONCERNING MARITIME PORT SECURITY

Jeffrey S. Olk  
Lieutenant, United States Coast Guard  
B.S., University of Phoenix 2002

Submitted in partial fulfillment of the  
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL  
March 2009

Author: Jeffrey S. Olk

Approved by: Alex Bordetsky  
Thesis Advisor

Michael Clement  
Second Reader

Dan Boger  
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Federal agencies that are within The Department of Homeland Security have many missions to support the security of the United States. One mission concurrent with this thesis topic is Maritime Interdiction Operations, which protects America's maritime borders from all intrusions by halting the flow of illegal drugs, aliens, and contraband into the United States through maritime routes. All government agencies within The Department of Homeland Security are continuing to focus their effort in sharing critical data to improve their situational awareness (SA) of command and control (C2), to make quicker decisions, and to collaborate with remote experts in support of another possible terrorist attack. Unfortunately this effort is being accomplished without the foresight of interoperability of existing databases throughout the agencies within The Department of Homeland Security.

The lack of interoperability of these databases between the agencies continues to be a major issue in the security and safety to our nation's maritime ports. This thesis will discuss the lack of interoperability of databases between federal, state and local law enforcement agencies. The need and urgency to collaborate these vital databases into one unified decentralized network—to store and retrieve critical information to protect our maritime ports of entry, when needed, to protect our nation from any possible future threats that may harm our nation—is also stressed.



THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

I.	EXPLORING INTEROPERABILITY OF DATABASES WITHIN DEPARTMENT OF HOMELAND SECURITY AGENCIES .....	1
A.	INTRODUCTION .....	1
B.	CURRENT PROBLEM .....	1
C.	STRENGTHING AMERICA .....	4
D.	BACKGROUND OF HOMELAND SECURITY .....	8
II.	DATABASES WITHIN DEPARTMENT OF HOMELAND SECURITY .....	13
A.	DHS PRIMARY INFORMATION SHARING NETWORK .....	13
1.	Description of System Database (HSIN) .....	13
2.	System Capabilities .....	16
3.	System Problems and Limitations .....	18
4.	Redesigning System Database to HSIN NextGen ..	20
III.	MARITIME INTERDICTION—ARE OUR PORTS SECURED? .....	23
A.	THE USE OF HOMELAND SECURITY DATABASES TO SUPPORT MARITIME PORT SECURITY .....	23
B.	THE CURRENT STATE OF PORT SECURITY WITHIN THE UNITED STATES .....	25
C.	MEGA-PORT INITIATIVE AND NUCLEAR RADIATION DETECTION. ....	28
D.	INFORMATION SHARING CRITICAL FOR MARITIME PORT SECURITY .....	30
IV.	CONNECTING THE DOTS .....	33
A.	CREATING A COMMON OPERATING PICTURE .....	33
B.	CREATING SITUATIONAL AWARENESS TO ENHANCE MARITIME PORT SECURITY. ....	35
C.	CHANGING POLICIES .....	39
D.	CHANGING MENTAL THOUGHT (RESISTANCE TO SHARE INFORMATION). ....	41
V.	DATA SHARING ENVIROMENT EXPERIMENT IN MIO 08-4 .....	45
VI.	CONCLUSION .....	57
A.	UNITY—SHARING THE SECRET .....	57
	LIST OF REFERENCES .....	63
	APPENDIX: SUPPORTING INTEROPERABILITY .....	69
A.	PRESIDENTIAL EXECUTIVE ORDER 13356 .....	69
B.	LETTER FROM HOMELAND SECURITY COMMITTEE .....	70
	INITIAL DISTRIBUTION LIST .....	73

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF FIGURES

Figure 1	Department of Homeland Security Agencies.....	12
Figure 2	Log on Screen into HSIN.....	14
Figure 3	Homeland Security Information Network.....	15
Figure 4	Homeland Security Fusion Center Locations.....	18
Figure 5	Example of container ship entering U.S. port.....	25
Figure 6	The Information Gap Theoretical Underpinnings of Situation Awareness: Critical Review by Mica R. Endsley.....	36
Figure 7	Diagram of the Theoretical Underpinnings of Situation Awareness: Critical Review by Mica R. Endsley.....	37
Figure 8	New Information Sharing Model from United States Intelligence Community Information Sharing Strategy.....	43
Figure 9	External view of target vessel (Container Vessel) pier side at Newark NJ Pier 17, September 8, 2008..	46
Figure 10	Sonar Alert biometrics from Demark seen in JSAS Situational Awareness Viewer Display screen.....	47
Figure 11	Streaming video frame (upper left corner) from NJSP vessel conducting search for small target vessels in Newark, NJ Harbor MIO.....	49
Figure 12	Small craft interdiction Groove Workspace MIO 07- 04.....	50
Figure 13	A Coast Guard RHIB off Manhattan on the morning of 11 September 2001 by Chan Irwin.....	62

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYNS AND ABBREVIATIONS

ANOA	Advanced Notice of Arrival
CAP	Common Alert Protocol
CBP	Customs and Border Protection
COI	Communities of Interest
COP	Common Operating Picture
CoT	Cursor on Target
COTP	Captain of the Port
CS	Critical Sector
CSI	Container Security Initiative
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNDO	Domestic Nuclear Detection Office
DOE	Department of Energy
EM	Emergency Management
FDNY	Fire Department New York
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
GDP	Gross Domestic Product
HSIN	Homeland Security Information Network
HSOC	Homeland Security Operations Center
IA	Information Analysis
IAEA	International Atomic Energy Agency
ICE	Immigration and Customs Enforcement
ID	Identification
IMO	International Maritime Organization
IND	Improvised Nuclear Device
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
ISPS	International Ship and Port Security
JRIES	Joint Regional Information Exchange System
JSAS	Joint Situational Awareness System
LE	Law Enforcement
LEO	Law Enforcement Online
LINX	Law Enforcement Information Exchange
MIO	Maritime Interdiction Operations
MTSA	Maritime Transportation Security Act
NextGen	Next Generation
NNSA	National Nuclear Security Administration
NOA	Notice of Arrival
NOC	National Operations Center
NPS	Naval Postgraduate School
NRC	National Capitol Region

NVMC	National Vessel Movement Center
NYPD	New York Police Department
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PANYNJ	Ports Authority of New York and New Jersey
PAPD	Pennsylvania Police Department
RDD	Radiological Dispersion Device
RISS	Regional Information Sharing System
RISSNET	Regional Information Sharing System Network
SA	Situational Awareness
SAFE	Security and Accountability for Every Port Act
SBU	Sensitive-But-Unclassified
SFI	Secure Freight Initiative
TNT	Tactical Network Topology
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism
USCG	United States Coast Guard
VIRT	Valuable Information at the Right Time

## **ACKNOWLEDGMENTS**

I would like to thank my family (Jennifer & Gabriella) for their patient and unselfish support showed during my studies at NPS and for the completion of this project as well.

Furthermore, I would like to thank and express my deepest appreciation to my thesis advisors, Dr. Alex Bordetsky, and Mr. Michael Clement for their guiding help. Lastly, I'm grateful to the faculty and staff of the Naval Postgraduate School for giving me the tools required to look at the world in a different way and for inspiring my belief that every problem has a solution if you just work hard enough at it.



THIS PAGE INTENTIONALLY LEFT BLANK

# **I. EXPLORING INTEROPERABILITY OF DATABASES WITHIN DEPARTMENT OF HOMELAND SECURITY AGENCIES**

## **A. INTRODUCTION**

Since Homeland Security was established in November 2002, the organization has encountered situations where the lack of effective interagency data sharing has resulted in failure to intercept attacks and secure our nation. Over the past eight years the President of the United States has issued numerous executive orders and memorandums mandating that the federal government implement an aggressive effort to ensure information sharing between federal, state and local agencies. Within these Executive Orders, the President is mandating to fully engage in the combined effort to embrace interoperability between fellow government agencies. The effort has been in full force since the aftermath of the September 11 terrorist attack and the catastrophic event of Hurricane Katrina.

## **B. CURRENT PROBLEM**

The Department of Homeland Security (DHS) and the U.S. Department of Justice have an ambitious plan to improve interagency exchange of intelligence among agencies across the United States. An example of this is the establishment of Data Fusion Centers in major urban areas. The Fusion Centers coordinate, gather, analyze, and disseminate law enforcement, homeland security, public safety, and terrorism information among federal, state, and local officials. The Data Fusion Centers were created in the aftermath of September 11 in an attempt to prevent the intelligence

failures that led to the attacks. Fifty-eight fusion centers have been established throughout the United States. In support of the effort to implement the information-sharing environment each of the fifty-eight fusion centers use a web-based information sharing application. Homeland Security Information Network (HSIN) is the primary means for communication, collaboration, situational awareness, and information sharing within DHS.

DHS anxiously deployed HSIN to all fifty states, five territories and Washington, D.C to meet the demand of the U.S. President's executive orders and memorandums. Because the initial version of HSIN (developed with Groove) could not meet the demand of its large increase of targeted audience, DHS decide to migrate HSIN to its web-based cube-like environments called communities of interest (COI). DHS's main role and objective was to introduce a system that would foster interoperability among federal, state, and local authorities to enhance counterterrorism throughout the United States. DHS was unable to implement such a system due to essential and effective planning. DHS rushed the HSIN schedule, did not clearly define relationships to existing systems, developed and deployed HSIN in an ad-hoc manner, provided inadequate user guidance and did not establish performance metrics (Wagner 2007).

All over the United States the fusion centers are still unable to share information as intended. The fusion centers that utilize HISN are not working as planned because many agencies that have access to HSIN act as if they are in the cold war state of mind where everyone has to safeguard their information. This leaves a nation that is very reluctant to

share information between agencies. Agencies tend to over classify their data, leaving no choice but not to share the data. There is no current incentive to share information throughout the agencies; instead you risk the chance of being penalized.

Eight years after 9/11, the inability to share critical information seamlessly between agencies still exists. There are many organized groups within the world that are very aware of the nations inability to share information and secure the maritime ports, terrorists are very aware of this unaddressed vulnerability. Terrorist are preparing in many ways to exploit our maritime ports; "Unfortunately, the question of whether terrorists will act to exploit the weaknesses in port security is, unfortunately, not a matter of 'if' they will, but 'when' they will." (Goslin 2008) Below are some examples the intelligence community has gathered revealing striking information of terrorist preparing for an event.

➤ When captured in November 2002, Abd al-Rahim al-Nashiri, Al Qaida's operations chief in the Persian Gulf had developed a four-pronged strategy to attack Western-shipping targets:

- Blowing up medium-sized vessels at ports
- Attacking vulnerable, large cargo ships such as super tankers from the air by using explosive-laden small aircraft
- Underwater attacks by divers or suicide demolition teams, using limpet mines

Al-Nashiri was an explosives expert, specializing in naval demolition sabotage (Eshel 2005).

- At least one Al Qaida operative is known to have been in the process of obtaining an international seaman's license that would allow him into any port in the world without a visa (Tyler 2002).
  
- In 2003, 35 heavily armed terrorists boarded a chemical tanker off the coast of Sumatra. However, unlike pirates who operate in the region and routinely rob the crew and loot the vessel, these boarders simply demanded that the ship's captain teach them how to 'drive' the large ship. Like the 9/11 hijackers, who only wanted to learn to fly an airliner, these boarders were not interested in learning how to dock the vessel (Tyler 2002).

This thesis will take a look at the background of the development of HSIN and problems concerning interagency data sharing and its current usage. This thesis will also highlight how Maritime Port Security is at risk due to the nation's inability to share intelligence. The author believes Maritime Port Security is a ticking time bomb that needs our urgent attention to avoid another unforgettable terrorist attack.

### **C. STRENGTHING AMERICA**

Listed below is an example of the extensive effort from the federal government intensifying its position to improve communications, collaboration, and information sharing between government and private sector agencies at all levels according to the Information Sharing Environment (ISE) government website.

- *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001* This act was passed largely by both the democratic party and the republican party which increases the ability of law enforcement to search e-mails, telephone, medical and financial records.
- *The Homeland Security Act of 2002* This act was the establishment of the Department of Homeland Security as an executive department of the United States. The primary mission of the department is to prevent terrorist attacks within the United States. The department is to reduce the vulnerability of the United States to terrorist attacks while minimizing the damage. The department will also assist in the recovery from terrorist attacks that do occur within the United States. The Homeland Security Act also states that the department will have a central part in improving the sharing of information among federal, state, local government agencies and the private sector.
- *The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)* was signed on December 17, 2004 and was divided into eight titles; Reform of the intelligence community, Federal Bureau of Investigation, Security clearances, Transportation, Security, Border protection & immigration, Terrorism prevention, Implementation of 9/11 Commission recommendations and other matters. This act ensures closer coordination of the integration of the 16 agencies that make up the

Intelligence Community. For example, IRTPA requires no air travel within the United States or abroad without prior government approval.

- The President issued Executive Order 13356, strengthening the Sharing of Terrorism Information to Protect Americans, August 27, 2004 that superseded Executive Order 13388. In this executive order, President Bush gives the highest priority to prevent terrorist attacks against the United States and the interchange of information among federal, state and local governments.

Further building on President Bush's vision to strengthen Information sharing among federal, state and local authorities, he established the Information Sharing Environment agency. This agency has the overall responsibility for implementation of Information sharing among the federal government agencies.

Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, embraced the key principles of Executive Order 13356 and directed the establishment of the Information Sharing Environment.

The President was charged to create the ISE, designate its organization and management structure, and determine and enforce the policies and rules to govern the ISE's content and usage. The law further required the ISE be "a decentralized, distributed, and coordinated environment" that "to the greatest extent practicable, connects existing systems; builds upon existing systems capabilities currently in use across the government; facilitates the sharing of information at and across all levels of security; and

incorporates protections for individuals' privacy and civil liberties (Information Sharing Environment n.d.).

On October 25, 2005, the President issued Executive Order 13388 revoking Executive Order 13356, Further Strengthening the Sharing of Terrorism Information to Protect Americans, to facilitate the work of the ISE's Program Manager, expedite the establishment of the ISE, and restructure the Information Sharing Council.

On December 16, 2005, in accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, the President issued a Memorandum to Heads of Executive Departments and Agencies prescribing the guidelines and requirements in support of the creation and implementation of the ISE. The Memorandum contained two requirements and five guidelines that prioritize efforts the President believes are most critical to the development of the ISE and assigned Cabinet officials responsibility for resolving some of the more complicated issues associated with information sharing among federal, state and local authorities.

The President directed that the ISE be established by building upon "existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively "resources") used for the sharing and integration of and access to terrorism-related information, and leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information (Information Sharing Environment n.d.).



#### D. BACKGROUND OF HOMELAND SECURITY

The United States Department of Homeland Security was established on November 25, 2002, by the Homeland Security Act of 2002 following the aftermath terrorist attacks of September 11, 2001. The creation of DHS constitutes the biggest reorganization of U.S. government in American history and the most substantial reorganization of federal government agencies in the fifty years since the United States Department of Defense was created. DHS also constitutes the most diverse merger of federal functions and responsibilities, incorporating 16 department components into a single organization. The following is a listing of major agencies that are now within Department of Homeland Security.

- **The Directorate for National Protection and Programs** Serves the public by providing knowledge, skills, and equipment to help secure the National critical infrastructure assets. The agency is able to assist in providing a risk-based approach that takes into account all hazards, threats, vulnerabilities, critically, consequences, and available mitigation strategies.
- **The Directorate for Science and Technology** is the primary research and development arm of the Department. It provides federal, state and local officials with the technology and capabilities to protect the homeland.
- **The Directorate for Management** The Directorate of Science and Technology is the primary organization for research and development in the Department of Homeland Security. The directorate consists primarily of six divisions:

Chemical and Biological; Explosives; Command, Control, and Interoperability; Borders and Maritime Security; Infrastructure and Geophysical; and Human Factors. Additional offices have responsibilities, such as laboratory facilities and university programs that cut across the divisions.

- **The Office of Policy** strengthens the security by developing and integrating department-wide policies in order to coordinate the departments prevention, protection, response and recovery missions. The Office of Policy bridges multiple headquarter components and operating agencies to improve communication among DHS entities.
- **The Office of Health Affairs** serves as the principal agent for all medical health matters for the Department of Homeland Security. The Office of Health Affairs role is to develop and support an intelligence-based bio-defense and health preparedness architecture to ensure the security of our Nation in the face of all hazards.
- **The Office of Intelligence and Analysis** has the responsibility of gathering information, assessing data and disseminating to the appropriate agencies. This data is used to protect the territory of the United States from terrorist attacks and responding to natural disasters.
- **The Office of Operations Coordination** has the responsibility for monitoring the security of the United States and coordinating activities that would prevent, protect, and respond from terrorist threats and man-made disasters. The office is focused on information sharing

through their National Operations Center (NOC) to deter, detect, and prevent terrorist attacks. The NOC uses a database named Homeland Security Information Network (HSIN).

- **The Federal Law Enforcement Training Center** provides training opportunities to state, local, and campus and tribal law enforcement officers at low or no cost, which will enhance their ability to enforce new methods while staying safe.
- **The Domestic Nuclear Detection Office's** main objective is to detect and report any unauthorized attempts to import, posse or transport any radiological material within the United States.
- **The Transportation Security Administration (TSA)** oversees the security for the highways, railroads, buses, mass transit system, ports and the airports. Their main focus is that these areas are safe for travel.
- **United States Customs and Border Protection (CBP)** main mission is to prevent terrorist from entering the United States while regulating and facilitating international trade, collecting duties and enforcing U.S. Trade Laws.
- **United States Citizenship and Immigration Services** oversees the immigration to the United States, which establishes policies and procedures.
- **United States Immigration and Customs Enforcement (ICE),** targets criminal networks and terrorist organizations that seek to exploit vulnerabilities in our immigration system.

- **The United States Coast Guard** is involved in maritime law enforcement, mariner assistance, search and rescue, marine inspections of U.S. /Foreign vessels entering the United States. The main mission is to protect the public, the environment, and the United States economic and security interests in America's ports, waterways and international waters.
- **The Federal Emergency Management Agency (FEMA)** has the responsibility to reduce the loss of life and property from natural disasters, acts of terrorism and man-made disasters.
- **The United States Secret Service** protects the President and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure. (Department of Homeland Security, n.d.)

As these agencies were merged into the Department of Homeland Security, each agency had their own independent database that was not designed to share information seamlessly with others. With the creation of the Department of Homeland Security, they were tasked with the responsibility of creating an interagency information-sharing environment to combat terrorism within the United States. This information-sharing environment will be designed to assist federal, state, and local law enforcement agencies in identifying possible threats against the United States by using existing data collect by all agencies. This

thesis will highlight how this information-sharing environment is linked to the security of our maritime ports of entry.

## U.S. DEPARTMENT OF HOMELAND SECURITY

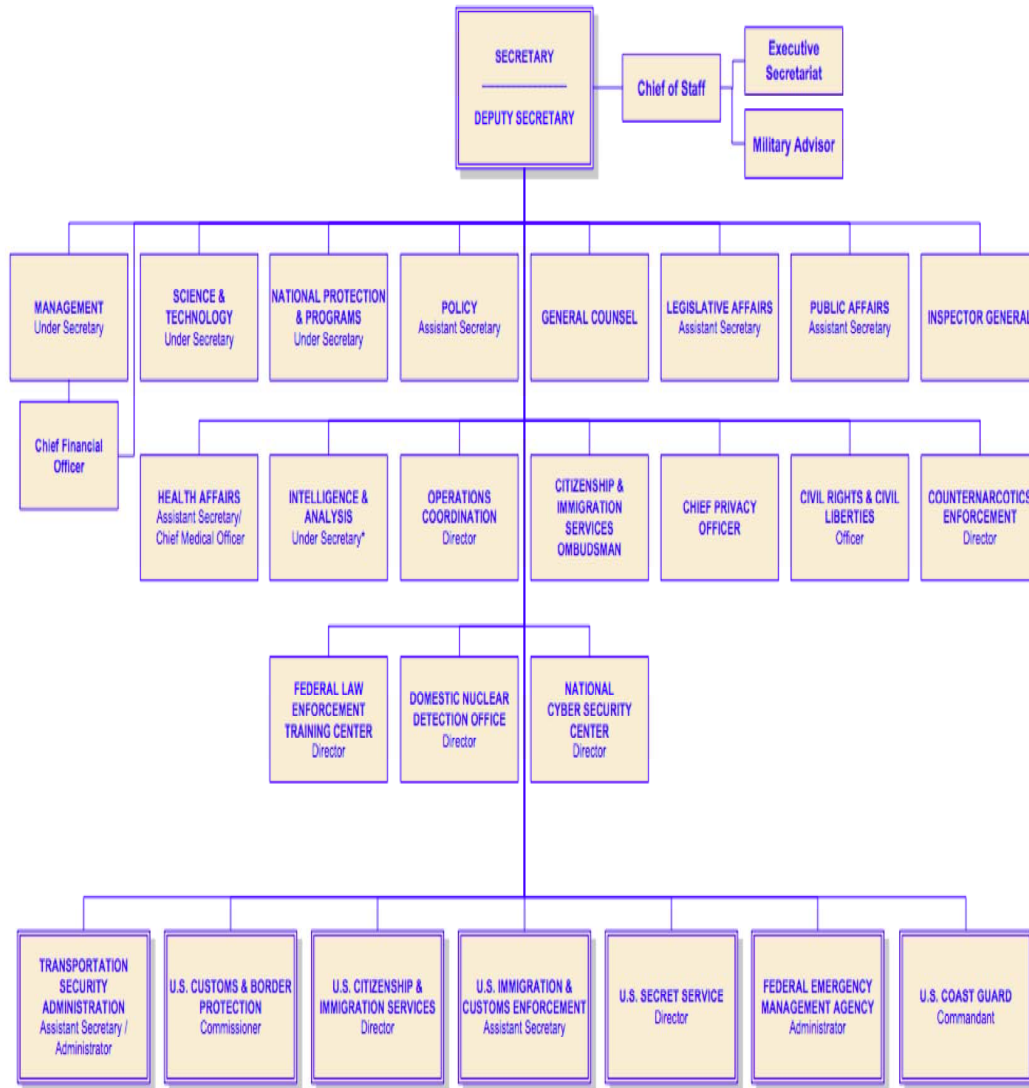


Figure 1 Department of Homeland Security Agencies.

## **II. DATABASES WITHIN DEPARTMENT OF HOMELAND SECURITY**

### **A. DHS PRIMARY INFORMATION SHARING NETWORK**

#### **1. Description of System Database (HSIN)**

The Homeland Security Information Network (HSIN) was first created as an extension of the Joint Regional Information Exchange System (JRIES), which started in 2002 as a pilot system to connect the California Anti-Terrorism Information Center, the New York Police Department, and the Department of Defense Intelligence Agency (DIA). This pilot system was designed to exchange real time intelligence and law enforcement data between the departments and assist in the detection of any possible terrorist activities in a secure environment. On September 2003, the DIA transferred ownership of the program due to funding constraints to the DHS. Upon receiving the program, DHS realized that they could vastly expand the current program beyond its current use to include the integration and interoperability of information sharing throughout federal, state, local, tribal authorities to prevent terrorism as undertaking incident management activities. To reflect the program's new scope of interest and abilities the department decided the program should be renamed to Homeland Security Information Network (HSIN).

The Office of Operations Coordination has the responsibility for monitoring the security of the United States and coordinating activities that would prevent, protect, and respond from terrorist threats and man-made

disasters. The office is focused on information sharing through their National Operations Center (NOC) to deter, detect, and prevent terrorist attacks. The NOC furthered the development of HSIN and designed the program to allow federal, state, local and tribal authorities to voluntarily add information for sharing to HSIN as needed, meaning no authority actually has a mandated requirement to submit information and users are allowed to access other relevant authorities information.

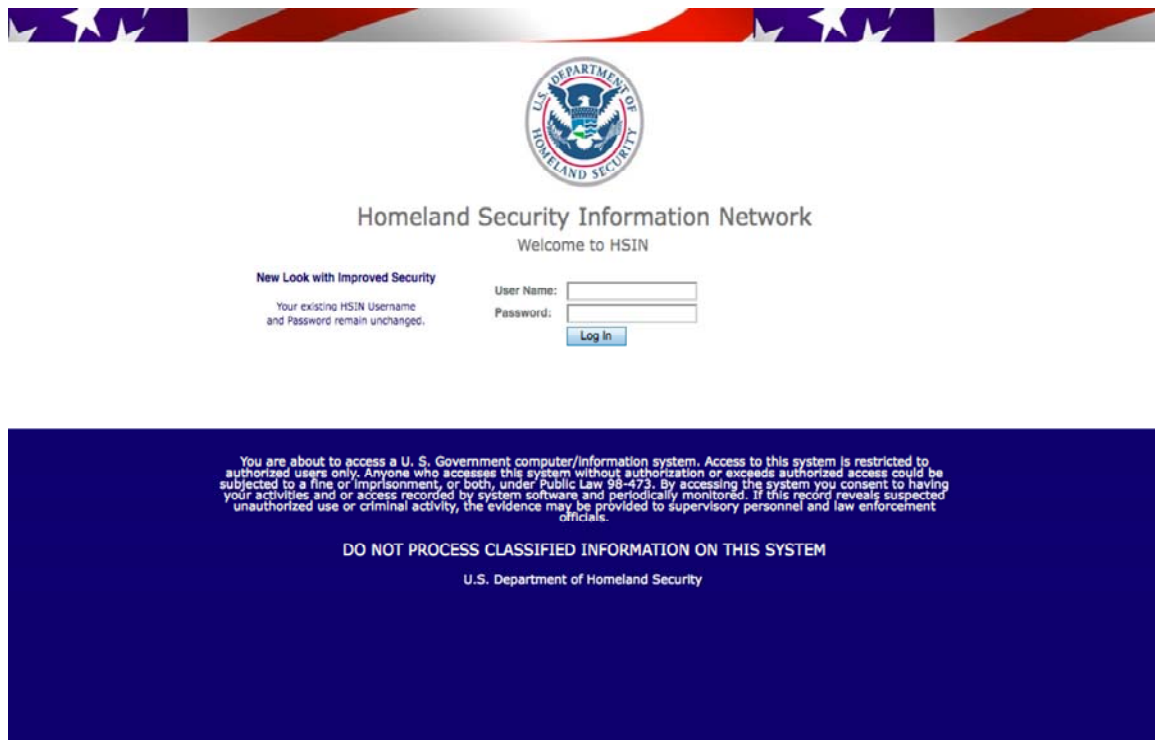


Figure 2 Log on Screen into HSIN.

To be able to voluntarily share information with relevant authorities the NOC established different COIs within the HSIN network. They include; HSIN National Operations Center (NOC), HSIN Law Enforcement (LE), HSIN

Government, HSIN Emergency Management (EM), HSIN Information Analysis (IA), HSIN National Capitol Region (NCR), HSIN International, HSIN Critical Sector (CS) and HSIN Congress.

## HSIN Structure

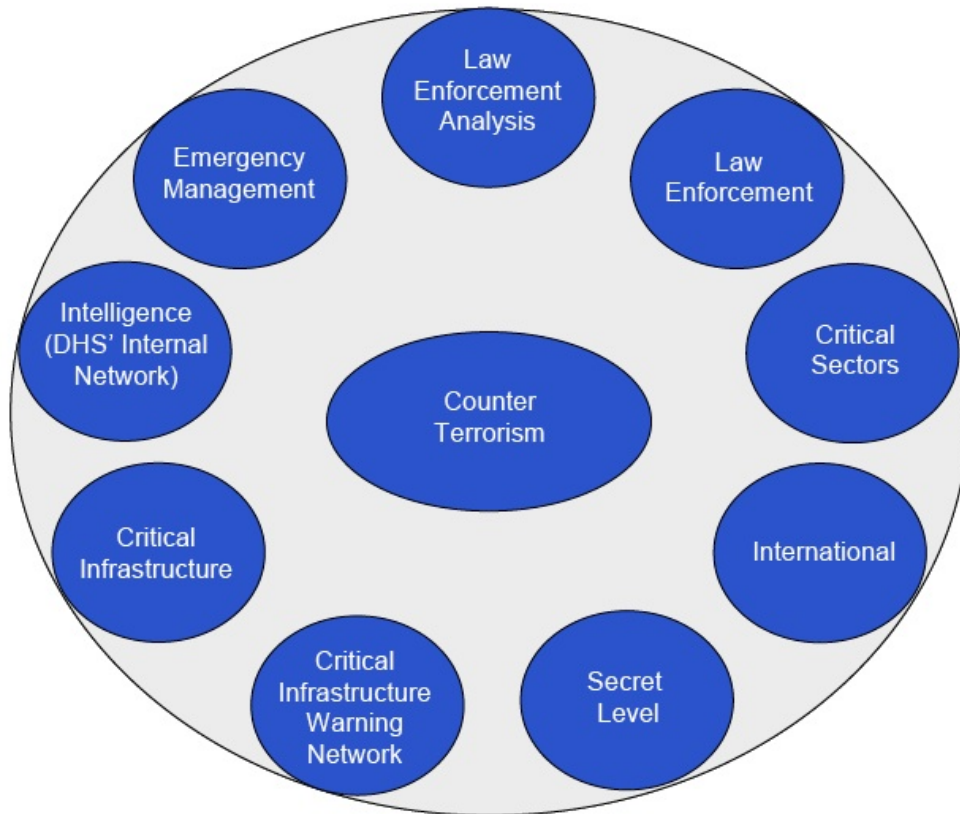


Figure 3 Homeland Security Information Network.

The HSIN COIs are collaborative cube-like environments where users within the same subject matter area or industry may voluntarily post and view information from others (if any added). The cube-like environment functions like a chat room where threads are posted and users post replies within that thread. The environment has other tools such as



instant chat to discuss with other users. However, each individual COI decides whether to enable these tools.

To gain access to this cube-like environment an individual must submit their biographical information and employment information. Once the individual is verified, the user is given access to his/her respective COI, i.e., law enforcement, emergency management; however, an individual may be a member of more than one COI if criteria are met.

DHS is not responsible or the custodian for the monitoring of information found within HSIN. However, DHS provides the communication tool for users to voluntarily add information for sharing as needed. (Operations Directorate National Operations Center 2007)

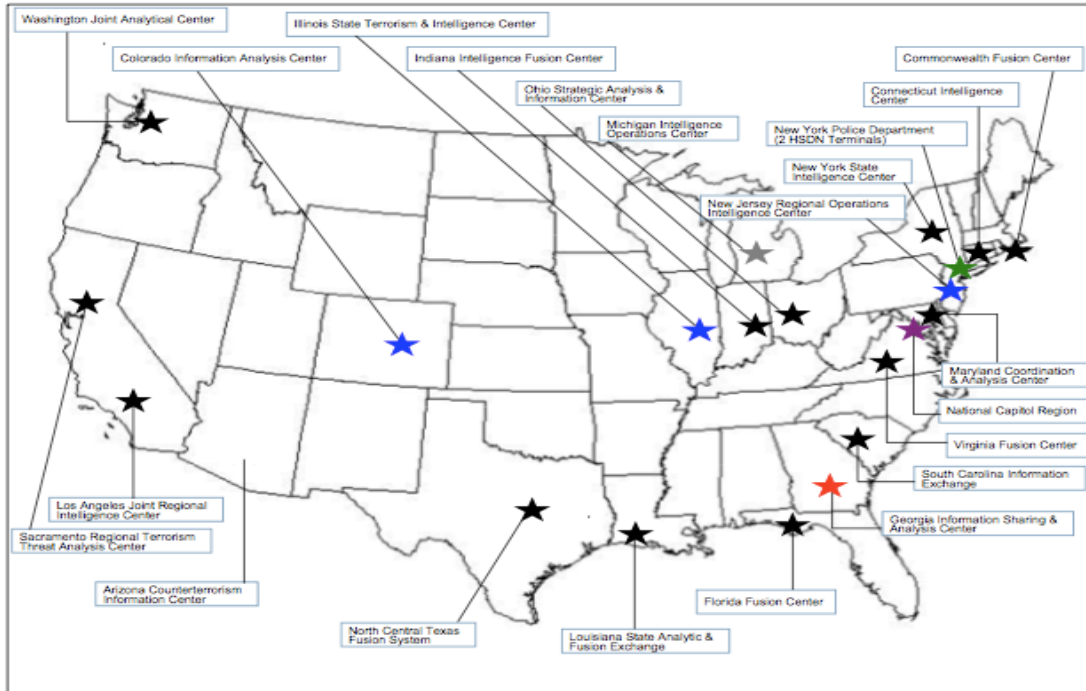
Also, the Department of Homeland Security reported to Congress in February 2008 that DHS has spent approximately \$69 million on HSIN over the past five years. The department has additionally report to Office of Management and Budget (OMB) and annual cost of \$21 million for the HSIN program for budget year 2008. DHS has halted further improvements on the existing HSIN system in September 2007. Since then, the department has only continued to operate and maintain the system. (Department of Homeland Security 2008)

## **2. System Capabilities**

The Homeland Security Information Network is a computer-based counterterrorism communications system connecting all fifty states, five territories, Washington, D.C and fifty major urban areas. HSIN is Department of Homeland Security secure, Sensitive-but-unclassified (SBU), web-based communications database that provides the primary

means of connectivity between the Homeland Security Operations Center (HSOC), the fifty-eight fusions centers throughout the United States along with federal, state, and local authorities.

HSIN is able to offer real time chat and instant messaging capabilities, as well as a document library that contains reports from multiple federal, state, and local sources. The system supplies suspicious incident and pre-incident information, mapping and imagery tools, 24/7 situational awareness, and analysis of terrorist threats, tactics, and weapons (Department of Homeland Security n.d.).



**I&A Resources at Fusion Centers**  
 3 Regional Coordinators, 19 Intelligence Officers, and 18 HSDN Terminals are installed in 22 locations.  
 Information is current as of March 2008.

- ★ Regional Coordinator, Intelligence Officer, HSDN Terminal Installed
- ★ Regional Coordinator, HSDN Terminal Installed, No Intelligence Officer
- ★ Regional Coordinator, No Intelligence Officer, No HSDN Terminal Installed
- ★ Intelligence Officer, HSDN Terminal Installed
- ★ Intelligence Officer, No HSDN Terminal Installed
- ★ HSDN Terminal Installed, No Regional Coordinator, No Intelligence Officer

Figure 4 Homeland Security Fusion Center Locations

### 3. System Problems and Limitations

Upon acquiring the system from the DIA in 2003, DHS was under pressure to expand the system to all federal, state and local authorities. With high concerns of possible future terrorist attacks, HSIN's strategy was to deploy the system to all federal, state and local authorities as it was and deal with the problems at a later date. The pressure DHS was receiving to implement a product created an atmosphere that did not produce a quality product for anyone to use

effectively (Deffer 2006). During DHS's hurried implementation, their delivery of the system overlooked the use and collaboration with comparable law enforcement systems such as, Law Enforcement Online (LEO) and the Regional Information Sharing System Network (RISSNET) resulted in duplication of data and opportunities for sharing (Deffer 2006.) Many law enforcement agencies still today use LEO and RISSNET over HSIN because of their ability to share information more efficiently, the one thing that HSIN was to replace. Also, DHS developed the Communities of Interest cube-like environment that only let communities of the same nature share information [National Operations Center (NOC), Law Enforcement (LE), Government, Emergency Management (EM), Information Analysis (IA), National Capitol Region (NCR), International, Critical Sector (CS)] leaving an environment that is not fostering the whole concept of interoperable information sharing among federal, state, and local authorities. Furthermore, DHS did not conduct a complete technical evaluation of HSIN before their implementation. There was inadequate user guidance, training, and reference materials discussing how and what should be shared among their communities of interest. This resulted in federal, state, and local authorities defining their own information sharing process, which increased duplication and lack of standardization.

Another concern is that DHS is not developing adequate performance measures. DHS measures its performance based on active user accounts throughout the federal, state, and local authorities. This is a poor measurement of how many individuals actually use HSIN on a daily basis to share information. HSIN has approximately 18,000 registered users

which only 6 percent contribute daily to the network's three major portals: law enforcement, emergency management, and counter terrorism; therefore HSIN has only about 1,100 active users. (Department of Homeland Security, OIG-06-38, 2006)

Due to HSIN's inability to link with other databases, such as LEO and RISSNET, and share information with other communities of interest, many users convey a large dissatisfaction of the functionalities that HSIN was supposed to address and fix. (Deffer 2006) At this point, many users do not understand HSIN's role in information sharing and do not trust the system's capabilities to meet their needs. Many users still use LEO and RISSNET to conduct their day-to-day business and share information with other federal, state, and local authorities. Some agencies have given up on HSIN and started developing their own ad-hoc stove-piped information sharing system that HSIN was intended to correct. (Deffer 2006)

With the development of alternative information sharing systems, users are making limited use of HSIN. Even though law enforcement is the principle customer, officials at fusion centers and counterterrorism units have said that they do not use HSIN to share information on a regular basis or do not log on at all to share information. (Deffer 2006)

#### **4. Redesigning System Database to HSIN NextGen**

In February 2008, DHS announced to its user (federal, state, and local authorities) that HSIN was going be upgraded to meet their suggested needs. The upgrade was named NextGen, which started its initial phase into the

authorities in May 2008. DHS has stated that this upgrade of HSIN to NextGen is to significantly increase information sharing among the authorities. DHS decided to upgrade the existing HSIN because the existing system had security concerns and information sharing throughout the between agencies were not being accomplished. Also, with the first version of HSIN, DHS has a key initiative to reduce the number of systems within DHS that share sensitive but unclassified information.

Along with the announcement of NextGen, DHS developed an acquisition strategy where the system will be implemented in four phases with additional users increasing with each phase. DHS will start to transition its current users of HSIN to NextGen in May 2009. DHS has awarded the contract to General Dynamics One Source, LLC of Fairfax, VA that will develop, deploy, operate and maintain the new system. The initial award will be for \$19 million and the total potential value if all four options are exercised is \$62 million. DHS will continue to use HSIN with a goal of retirement in September 2009 when HSIN NextGen is expected to be completed. DHS estimates it has spent a total of \$91 million on the current HSIN through fiscal 2008. Also, to continue to operate HSIN until September 2009, DHS has estimated that it will spend an additional 3.1 million. [From the learning curve of the existing version of HSIN], DHS still is in the process of identifying sound controls such as project and acquisition planning, requirements development and management and risk management to fully and effectively manage HSIN NextGen in a closely controlled manner. DHS plans to address these weaknesses by tasking

the contractor to assist in the development and completion in the risk management area. (Department of Homeland Security, OIG-09-07, 2008)

Until these weaknesses are effectively addressed and DHS implements and institutionalizes the full set of acquisition management controls, the project will be at increased risk of operating in an ad hoc and chaotic manner—potentially resulting in increased project costs, delayed schedules, and performance shortfalls. (Department of Homeland Security, OIG-09-07, 2008)

### **III. MARITIME INTERDICTION—ARE OUR PORTS SECURED?**

#### **A. THE USE OF HOMELAND SECURITY DATABASES TO SUPPORT MARITIME PORT SECURITY**

The nation we live in is ever changing and the conventional thinking has failed to adapt to a world of new threats. Today we live in a technology enriched environment where we are able to stay connected and get the information we are requesting with the touch of a button. So the question has to be asked, "why doesn't the United States have a functional database to combat terrorism"? Even after the Government Accounting Office, The Department of Homeland Security Inspector General and a Congressional Research Service for Congress have all stated in several reports that the agency has been unable to create a fully functional interoperable network that can be used by all agencies to strengthen the nations ability to combat terrorism, nothing improves. These reports also provided strong recommendations for attending to their oversight. Here we are eight years later and we still do not have what we need to keep America safe. Maritime Ports throughout America are ticking time bombs that are just beginning to be addressed. One major contributor to the success of protecting our Maritime ports is the ability to share intelligence seamlessly with other federal, state and local agencies. There are several databases currently in use around DHS agencies that address Maritime Port Security. CBP has a database named ACE and PRIDE while the Coast Guard has MISSLE and the newly constructed WATCHKEEPER. All these databases contain intelligence on incoming vessels, containers, and the



Maritime Port Security agreements with the local ports throughout the nation. Moreover, all these databases are completely independent of each other with no way to share critical intelligence if needed in support of another terrorist attack.

Many of the efforts to protect our maritime ports are duplicated by multiple agencies while wasting resources and time that could be better utilized. For example, CBP will attend to a foreign vessel calling on a U.S. port to conduct an inspection and validate the individuals on board or to check the validity of the claimed cargo on board the vessel. As CBP is leaving the vessel with their collected information, the Coast Guard is boarding the vessel to obtain the same information that CBP just ascertained. The inefficiency of not having an interoperable intelligence-sharing network is completely unacceptable in the era we live. The Maritime Port Security is at the hands of the Department of Homeland Security, which has a responsibility to safe guard America and provide an intelligence-sharing platform.

**B. THE CURRENT STATE OF PORT SECURITY WITHIN THE UNITED STATES**



Figure 5 Example of container ship entering U.S. port.

The terrorist attack of September 11, 2001 on the United States has heightened the security of all elements not excluding Maritime Port Security. With 70 percent of the planet covered with water, ships carry approximately 80 percent of the world trade by volume. (United Nations Conference on Trade and Development, 2002) The United States has 361 ports and 95,000 miles of coastline. While the United States leads the world as the leading trading nation, accounting for nearly 20 percent of the annual world ocean-borne overseas trade. The 6 million cargo vessels that enter the United States account for 25 percent of the Gross Domestic Product (GDP) (Frittelli 2005).

On November 25, 2002, congress established a new port security framework named the Maritime Transportation Security Act (MTSA). The MTSA is the United States version of the International Ship and Port Security (ISPS) Code issued from the International Maritime Organization (IMO).

MTSA was developed to aide in the protection of the nations ports and waterways. Within the MTSA there were a series of security improvements in the ability to conduct assessments of port facilities and vessels; the ability to identify risk associated with ports and be able to write security plans that reflect these concerns; the development of the Transportation Worker Identification Credential (TWIC) which is a controlled access secure biometric ID card for port works to access identified restricted area's; also an evaluation of foreign ports from which United States bound vessels may depart.

Another step forward in the nation's security was the creation of the Security and Accountability for Every (SAFE) Port Act 2006. The SAFE placed new procedures and amended a few MTSA regulations while increasing maritime security. The SAFE act developed a comprehensive timetable and set fee restrictions for the TWIC; also the Container Security Initiative (CSI) which will process and examine containers that are loaded at foreign ports before they enter the United States.

The United States Coast Guard (USCG) and the Bureau of Customs of Border Protection (CBP) are the primary departments within the Department of Homeland Security that have the ultimate responsibility for securing our Nations Ports.

The Coast Guard is the nations premier maritime law enforcement authority, which recently under the MTSA act was empowered with the nations port security issues. The Coast Guard has a vast amount of responsibility in intercepting terrorist threats associated with foreign vessels aimed at

our U.S. ports. To foster this initiative, the Coast Guard sought to improve the overall quality of information that was being supplied by foreign vessels entering the United States. The Coast Guard instituted new reporting requirements for vessels entering and departing the United States under the former 24-hour advanced Notice of Arrival (NOA). The new requirements under the Advanced Notice of Arrival (ANOVA) require vessels entering the United States to enter complete information on the vessels crewmembers, passengers, cargo and general characteristics of the vessel (i.e. IMO ship identification number, ISPS security plan completed) 96 hours before entering the United States. The Coast Guards National Vessel Movement Center (NVMC) receives all ANOVA and processes all submissions. Each Captain of the Port (COTP), however, has the ultimate responsibility for ensuring each ANOVA is complete for vessels entering their specific port of entry. The Coast Guard has issued numerous COTP orders denying the entry of foreign vessels into the United States because the vessel did not give their 96 ANOVA or had incomplete vessel data.

Custom and Border Protection main mission is to prevent terrorist from entering the United States while regulating and facilitating international trade, collecting duties and enforcing U.S. Trade laws. CBP working along side the U.S. Coast have their own vast amount of duties and responsibilities to protect our ports. CBP's Container Security Initiative (CSI) is an amazing effort to deter terrorist activity against the United States by allowing CBP agents to screen containers at foreign ports before the containers enter a U.S. waters. Along with this effort CBP increase their reporting of required information to be

submitted to the agency 24 hours before the cargo is to be loaded from a foreign port that is U.S. bound. Before the increase in submitting the required information the foreign vessel did not have to declare what they were carrying until they reached a port within the United States. CBP will no longer accept general terms such as general cargo for entry into the United States. Foreign vessels bound for the United States now have to specifically identify what chemicals or certain dangerous cargo may be present on the vessel. This enables CBP to focus more of their energy on high interest vessels coming into our ports that could be carrying nuclear radiological chemicals (Frittelli 2005).

### **C. MEGA-PORT INITIATIVE AND NUCLEAR RADIATION DETECTION**

The world's largest and busiest ports are considered Mega-ports, which provide terrorist a global shipping network for possible smuggling of radiological material. The purpose of the Mega-port initiative is to screen containers regardless of their destination, for nuclear and other radioactive material that could be used against the United States or its allies such as a dirty bomb<sup>1</sup>. The International Atomic Energy Agency (IAEA) noted that between 1993 and 2004, there were 650 confirmed cases of illegal trafficking of radiological materials worldwide. (International Atomic Energy Agency, 2004) Many of these materials that were found could have been used to make a

---

<sup>1</sup> A dirty bomb is a conventional explosive device with radioactive material wrapped around it. Detonating the device disperses the radioactive material, contaminating the area with radioactivity that can be difficult to clean. Dirty bombs are also known as radiological dispersion devices, CRS Report for Congress, Port and Maritime Security: Background and Issues for Congress, updated May 10, 2005 by John F. Frittelli.

nuclear weapon of a dirty bomb. The inability to identify and prevent the entry of any radiological material into the United States could have devastating consequences to the nations economic stability. The federal government has adapted a recommendation from 9/11 Commissions Act that will require 100 percent screening of all United States bound containers from foreign ports for radiological material using nuclear radiation detection by 2012.

Through the Mega-ports initiative the Department of Energy (DOE) is working with foreign governments to provide the Mega-ports with the nuclear radiation detection. Currently there are 75 ports, which are identified as a Mega-port initiative. According to the National Nuclear Security Administration (NNSA) "since the start of the Mega-ports Initiative in fiscal year 2003, NNSA has completed installations at 19 ports in various countries: Bahamas, Belgium, Colombia, Dominican Republic, Greece, Honduras (Secure Freight Initiative (SFI) Port), Israel (Pilot Project), the Netherlands, Oman, Pakistan (SFI Port), Panama, the Philippines, Spain, Singapore, South Korea (SFI Port), Sri Lanka, Thailand, and the United Kingdom (SFI Port). Implementation is underway at additional ports in more than 20 other locations, including: Bangladesh, Belgium, China, Djibouti, Dubai-United Arab Emirate, Egypt, Hong Kong, Israel, Jamaica, Japan, Malaysia, Mexico, Oman, Panama, Portugal, Spain, and Taiwan" with latest addition of Israel's Haifa Port, one of Israel's busiest seaports."

The Mega-port initiative and nuclear radiation detection is a giant step in the right direction of maritime port security. However, it is still unclear how the data

will be maintained or shared throughout Department of Homeland Security interagency. The federal government has many ongoing efforts to increase maritime port security of the nation but continues to lack a sustainable information-sharing interagency environment (U.S. Government Accountability Office 2007).

**D. INFORMATION SHARING CRITICAL FOR MARITIME PORT SECURITY**

The initiatives that are being taken by U.S. Coast Guard and Customs and Border Protection are important steps in building an effective foundation that will support maritime port security. However these initiatives alone are not fulfilling the nations deserving security (Frittelli 2005).

Information sharing among federal, state, local, tribal, private sector commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism to the United States is supposed to be one of Department of Homeland Security's main objectives. Maritime port security has increased since 9/11, but we still have large vulnerabilities relating to our inability to share critical information that could potentially secure our maritime ports. Since our attack on the United States we have rushed to secure our nation by developing information sharing networks that are no more useful today than they were eight years ago. The Department of Homeland Security was under such pressure to develop an information-sharing network immediately following 9/11 that the agency introduced HSIN. The system was introduced in such a rush that the agency was going to address operational problems

and details at a later date. The Departments of Homeland Security's HSIN network was introduced in 2003 and the agency has spent around 91 million dollars of federal monies to develop a network only 6 percent of its registered users find useful. Information sharing is the very foundation that is needed to secure our maritime ports. In maritime port security there are many different law enforcement agencies that have responsibilities contributing to the overall success of the detection and prevention of another terrorist attack on the United States. However, information sharing is at a bare minimum because we the government have been unable to develop an effective inter-linking network that is well accepted and used by all federal agencies to combat terrorism. Agencies all over the United States are duplicating their work efforts by not sharing critical information. Duplication of work and not sharing any data collected is where we were when 9/11 happened and we're still in the same situation. Duplication of effort by our federal agencies not only hampers our efforts to effective information sharing, but also hampers our efforts to secure our maritime ports form future terrorist activity and attack according to a testimony by Captain William Harris on Homeland Security Information Network to the U.S. House of Representatives.

Intelligence is the key element when detecting terrorist activity within a maritime domain. Being able to pin point exactly what vessel to intercept is going to require identifying precise intelligence. The only way the government is going to achieve this level of cohesiveness is to leave behind the idea of safe guarding information and enter the new era of sharing intelligence between agencies.



Currently, information sharing throughout the federal government still entertains the idea of disparate databases to secure our maritime ports.

For example, information such as last port of call, crew list and cargo are not currently being shared between CBP, USCG, ICE, etc. Each agency requires the foreign vessel to submit their information on specific forms. The process of vetting a vessel takes time, something that is not always available when dealing with terrorist activities. Information sharing between agencies is so vital in detecting future threats to our maritime ports of interest. The United States receives thousands of foreign vessels daily that have to be verified before entry. If we were able to collaborate information collected from each agency, we would have a higher probability of terrorist detection.

## **IV. CONNECTING THE DOTS**

### **A. CREATING A COMMON OPERATING PICTURE**

The ultimate goal in protecting our Maritime ports is the ability to share intelligent information between agencies that will enable a common operating picture (COP). The COP is a single identical display that is used by more than one decision authority to facilitate collaborative planning with an end result of decision superiority. If agencies are not using a COP they run the chance of miscommunication because they have different pictures, ideas and perspective of an event. The common operating picture is a virtual operating environment that promotes information sharing throughout federal, state, and local law enforcement authorities by giving each agency access to the information they need visually to effectively protect Maritime ports of entry.

Agencies throughout the Department of Homeland Security have different responsibilities that relate to protecting the security of our maritime ports. This includes Custom and Border Protection, United States Coast Guard, local police and fire departments to name a few. These separate agencies have tendencies not to communicate as often as they should which result with inconsistent systems supporting the processes of safeguarding maritime ports. An interoperable COP will allow multiple agencies to share information, while creating greater operational effectiveness in protecting our maritime ports. Also, by creating a COP, it reduces costs that would often result from maintaining disparate systems

across all agencies. The creation of a COP must ensure the environment is interoperable with the tools and process that these agencies are custom to using. Most of the time COP's are developed with the vision of only military or federal in mind with no consideration of our first responders. So we must ensure that our COP incorporates interoperability functionality to support both federal and first responders to be successful.

Once the COP is developed there are system privileges that can be set to allow access to specific user requirements. Being able to adjust the level of permissions an individual will have access to makes the COP scalable and secure. For example, the United States Coast Guard has information on vessels arriving into New York, however the fire department in San Diego, CA does not need this information to prevent/respond to and maritime port incident the Sand Diego area. So the COP is designed to limit access to some data to protect privacy and some military information may require a security clearance.

While we are in the process of creating an environment that accepts information sharing instead of safeguarding valuable information, technical solutions already exist and are waiting. Additionally, presidential memorandums are in place to support and enable interoperability. We are at a place in time now to embrace and move forward, and we can do this by eliminating our disparate systems and get on the same page by using a common operating system that will enhance the protection of or Maritime ports. (Pellicci n.d.)

## **B. CREATING SITUATIONAL AWARENESS TO ENHANCE MARITIME PORT SECURITY**

Now that we are on the path to interoperability and sharing information, we must have situational awareness (SA). Situational awareness is the process of knowing what is going on around oneself and being able to interpret what is important to the task at hand. There are three distinct levels of awareness: perception (level 1), comprehension (level 2) and projection (level 3) (Endsley et al. 2006, 634). With the movement through the machine age, the computer age and now the information age we have created tools that are no longer simple; we've moved into a complex information world. The systems today are capable of producing vast amount of information, both from internal and external environments. This is an amazing achievement to be able to locate, track and identify vessels entering any port in the United States. However, the problem is not the lack of information but finding what is needed when it is needed. There is a huge gap between the amounts of data being produced and disseminated and people's ability to find the key piece of information needed to maintain the security of maritime ports throughout the United States (Endsley et al. 2006).

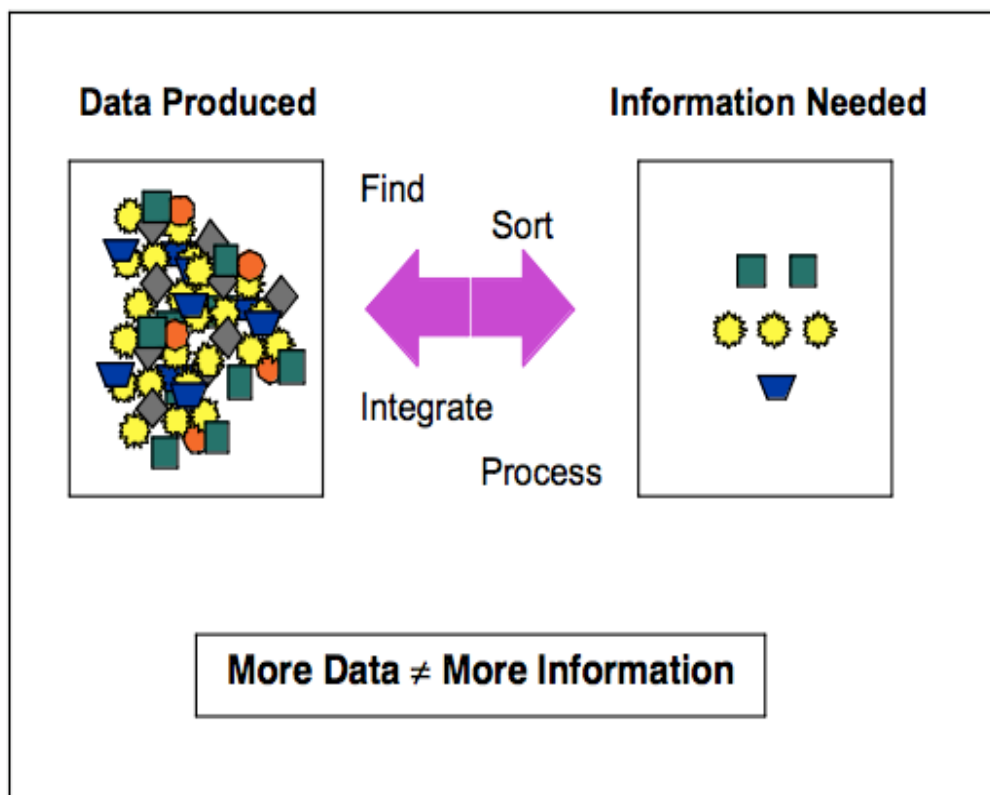


Figure 6 The Information Gap Theoretical Underpinnings of Situation Awareness: Critical Review by Mica R. Endsley

For example, information sharing between agencies is so important to success in fighting terrorism in the United States. However, there is a point where sharing too much information could be detrimental to your operational success. Have you ever received information that you requested and decided that it was just too much for what you needed? so you did not read anything at all. There is a concept that was developed by Dr. Hayes-Roth called Valuable Information at the right Time (VIRT). Information sharing has to be organized, managed and disseminated in a matter that individuals are not overwhelmed.

A general definition of SA that has been found acceptable across platforms describes SA as "the perception of the elements in the environment within a volume of time and space, the comprehension of the meaning and the projection of their status in the near future" (Endsley et al. 2000). This definition helps establish what "knowing what is going on" entails.

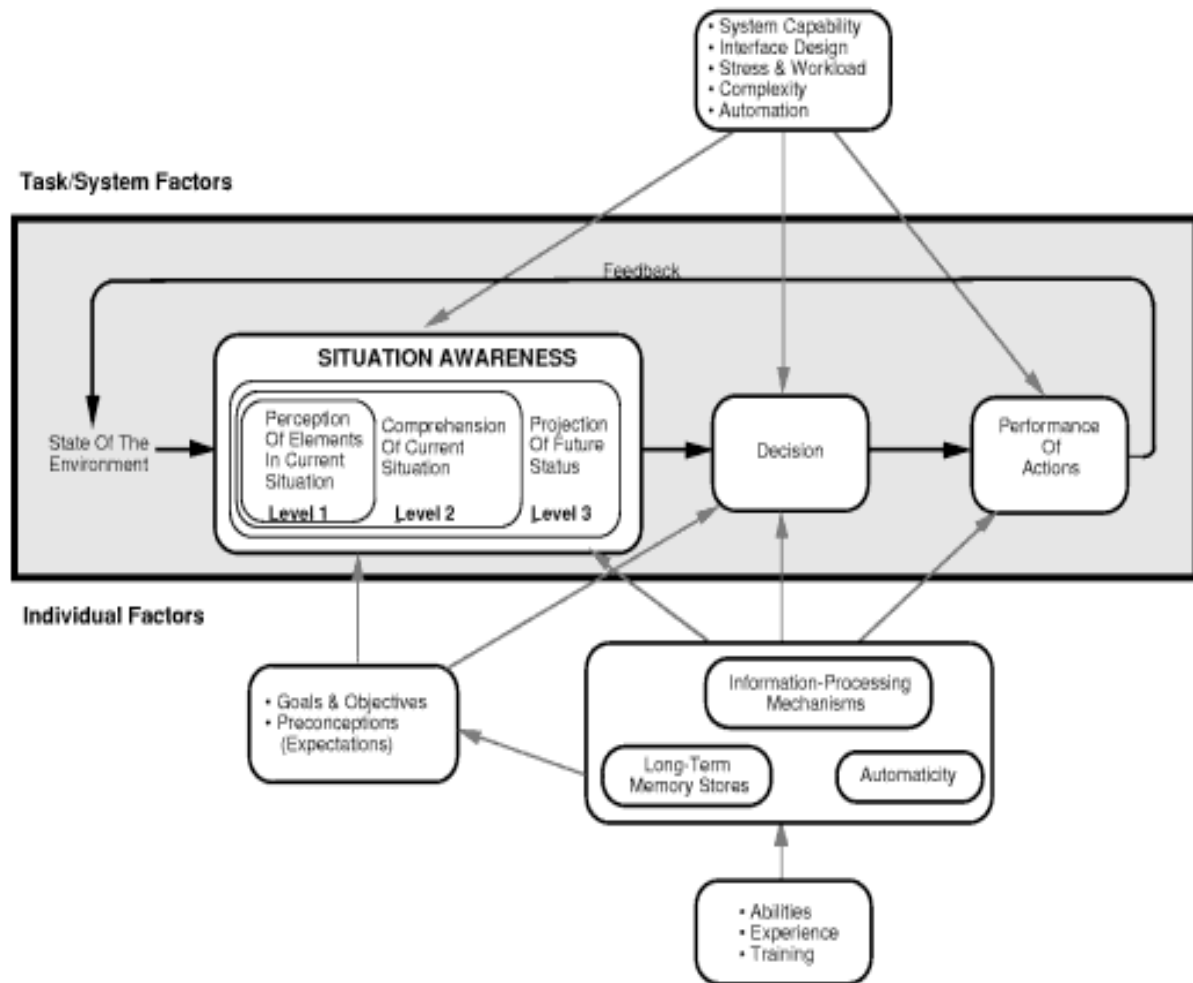


Figure 7 Diagram of the Theoretical Underpinnings of Situation Awareness: Critical Review by Mica R. Endsley

- Perception Level 1 - "The perception of relevant information from the environment forms the first level of SA. Without basic perception of important information (through visual, auditory, tactile, or other means), the odds of forming an incorrect picture of the situation increase dramatically. In highly complex and demanding environments, novices may have significant difficulty in knowing which information is most important or in accessing needed information is a timely matter to form level 1 SA".
- Comprehension Level 2 - "Situation awareness involves more than simple perception of information - it also demands that people understand the meaning and significance of what they have perceived [Level 2 SA]. Thus it encompasses how people combine, interpret, store, and retain information, integrating multiple pieces of information and arriving at a determination of its relevance to the person's goals. This analogous to having a high reading comprehension, as compared to just reading words".
- Projection Level 3 - "At the highest level of SA, the ability to forecast future situation events and dynamics [level 3 SA] marks individuals who have the highest level of understanding of the situation. This ability to protect from current events and dynamics to anticipate future events (and their implications) allows for timely decisions making. Experts rely heavily on future projections as hallmarks of skilled performance." (Endsley et al. 2006)

The SA model above represents how SA develops over time considering decision-making and performance. There are important enabling attributes within an environment that affect how people are able to obtain and maintain Situational awareness. These attributes include system

capability, design of system, system complexity, system automation and stress/workload because both of these decrease SA.

SA is an important key to enhancing Maritime Security throughout the United States. We must understand the interoperable systems we produce do not provide the SA nor do they create any need for SA in and of themselves, humans are the key to perception and decision-making.

For example, HSIN is an environment that was established for centralized information sharing. In this environment federal, state, and local authorities have the capability to freely added information if desired. CBP may discover that an incoming foreign vessel from South Africa has a high interest crewmember on board and decide not to share within HSIN, (since there is no mandate you have to share). By not sharing this critical information you are limiting the SA of the Coast Guard, ICE and local law enforcement authorities. Not sharing information weakens the decision makers ability to formulate a perception of acting on the information or not.

### **C. CHANGING POLICIES**

Currently the United States Government is constructed to win wars of the past by safe guarding their information and not sharing with other agencies. To be successful in preventing future terrorist attacks greatly depends on our ability to gather, analyze and share intelligence within federal agencies.

For the past eight years, the federal administration has set forth numerous changing policies to enhance and



mandate interoperability among federal, state, local and tribal agencies throughout the United States. The USA Patriot Act of 2001 and Presidential Executive Order 13356 are just a few examples that represent an effort to set information sharing standards and to enhance the overall security of our nation. Setting and changing policies is the first step towards creating a stronger informed nation. However, many of these policies are so radical to past beliefs of protecting information that after eight years of policy setting, we still do not have a framework fully capable of information sharing among all federal agencies. During the past eight years the federal government has made progress towards the goal of interoperability and sharing intelligence to combat terrorism, however, too many years have past with little success. The American people deserve more from their tax paying dollars that goes into developing interoperable software.

The federal government created the Department of Homeland Security in the aftermath of 9/11 to secure our nation and preserve our freedom. The agency also has the responsibility of creating an interoperable environment where vital data can be shared. In this thesis, I decided to highlight and examine the Department of Homeland Security's information sharing platform named HSIN. As mentioned earlier in this thesis, the development of HSIN has encountered many difficulties implementing the new policies to share information. The Department of Homeland Security is not the only federal agency having difficulties adjusting to policy change. The rush to establish an interoperable sharing environment is present throughout the

federal, state, and local governments. Just recently President Obama issued a new Presidential memorandum stating:

The government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears. In the face of doubt, openness prevails.

We are still in the process of accepting these needed changes set forth by the presidential memorandums. Maybe just setting a policy is not the answer to prepare us for another terrorist attack; maybe we need to change our mental thought of a "need to know" era to a "need to share" era.

**D. CHANGING MENTAL THOUGHT (RESISTANCE TO SHARE INFORMATION)**

In an effort to investigate the events leading to the attack on the World Trade Center, the 9/11 commission was formed. The commission issued a report stating that information sharing was one of the leading causes that lead to the inability to stop the attack. Regardless of the 9/11 commissions report highlighting serious oversight of sharing information many federal agencies still are trying to tackle the idea of sharing information between agencies.

In 2005, GAO placed information sharing on its high-risk list of government programs that face significant management problems, and it remains there today. GAO's latest high-risk report, released in January 2009, concluded that while agencies are developing an "information sharing environment, the scope, projects and milestones - - the roadmap -- for guiding the future [information sharing environment] were not fully defined" and, along with OMB, observed that "the

expected results and metrics -- the system of accountability -- to ensure progress were not in place. (Holmes 2009)

While policy setting improvements helped jump start the changing vision of enabling information sharing, policy setting alone is not enough to get the point across that information sharing is vital to our 21<sup>st</sup> century success on terrorism. The goal is to enable today's decision makers with the ability to understand completely the importance of changing their mental thought about sharing our vital information between agencies. Policies might be provided, but if you do not get the buy in from your stakeholders that hold the power to actually deploy the ideas behind the policies we will continue to live in an era of stove piped systems and just wait for our next attack. Or, we can take our decisions makers by the hand and give them the mental tools to envision what could be possible if interagency information sharing occurred on a daily basis. Changing mental thought of information sharing will not be easy because we have operated for so many years as independent entities of the United States government. Holding onto your information gives you and your agency power over others, job security, and an intellectual advantage. These are the type of decision makers we do not need working for our federal, state and local law enforcement authorities any longer. Our adversaries are monitoring our efforts and evolving rapidly in their motivations, we must move faster to provide a shared vision that will enable information sharing. The figure below is from the United States Intelligence community Information Sharing Strategy, which I think,

represents where we are and what we need to achieve to transform our nation into a truly unified information sharing nation.

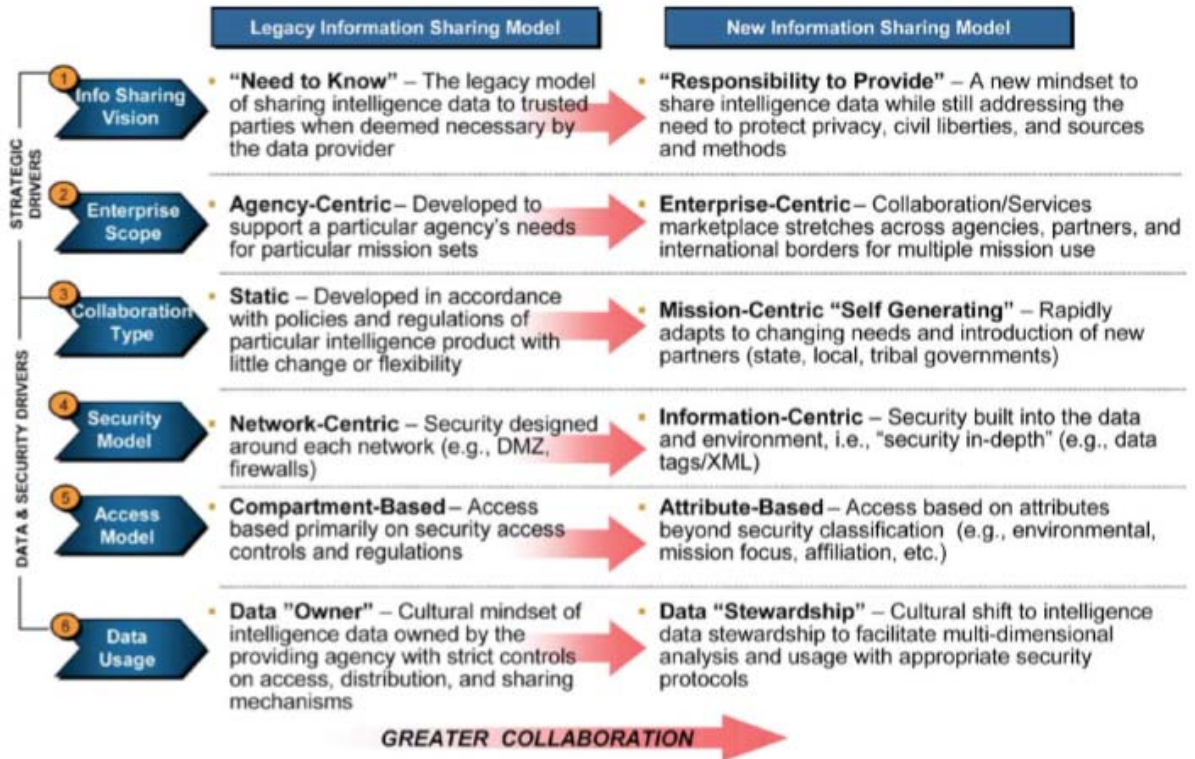


Figure 8 New Information Sharing Model from United States Intelligence Community Information Sharing Strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. DATA SHARING ENVIROMENT EXPERIMENT IN MIO 08-4

The Maritime Interdiction Operations (MIO) 08-4 experiment, which was conducted in September 8-12, 2008 in New York-New Jersey, Ft. Eustis, Sweden, Denmark to evaluate and test the use of networks, advanced sensors and collaborative data sharing for the rapid MIO. This experiment demonstrated the situational awareness focus and explored the requirements for interagency collaboration and data sharing. This experiment used the capabilities of Ports Authority of New York and New Jersey Joint Situational Awareness System (PANYJS JSAS), Microsoft GROOVE and the Naval Postgraduate School (NPS) situational tools.

In the following paragraphs there are portions of the TNT MIO 08-4 after action report along with the author's analysis, see (Bordetsky 2008) for the complete report.

This experiment will demonstrate that a decentralized network incorporating several data sources from around the world was used in collaboration for detection and interdiction. Agency participates were granted access based on their specific need to know criteria. This was a control security measure, which provided protection to certain vital information found within JSAS, GROOVE & NPS situational tools. However this detention and interdiction does not go without errors and highlights areas for improvements in data sharing among the interagency command structure.

On September 8, 2008 interagency partners in Europe indicated a possible threat by posting an alert in JSAS that a terrorist group had intentions of smuggling improvised nuclear device (IND) and radiological dispersion device

(RDD) into the United States, which was concealed in the cargo within a foreign flagged vessel heading for New York/New Jersey. This indication in JSAS was noticed by all local law enforcement agencies such as USCG, CBP, Port Authorities, PAPD, FDNY and NYPD prompting a massive collaboration effort to detect and interdict the vessel.



Figure 9 External view of target vessel (Container Vessel) pier side at Newark NJ Pier 17, September 8, 2008

Law enforcement officials conducted a boarding with hand held radiological detection equipment. During the boarding each agency had connectivity with JSAS, GROOVE & NPS SA and entered information upon detecting any radiological sources. The information was also being sent to

the Domestic Nuclear Detection Office (DNDO) for real time identification of the radiological material. The connectivity that the boarding teams had with JSAS, GROOVE & NPS SA tools facilitated the updating of the command and control centers by enabling situational awareness to the decision makers. Also during this boarding the teams were collecting a comprehensive crew list, last port of call data, biometrics (latent prints/facials) and were seamlessly sending real time voice and data through JSAS, GROOVE & NPS to all Command and Control Centers through out the world.

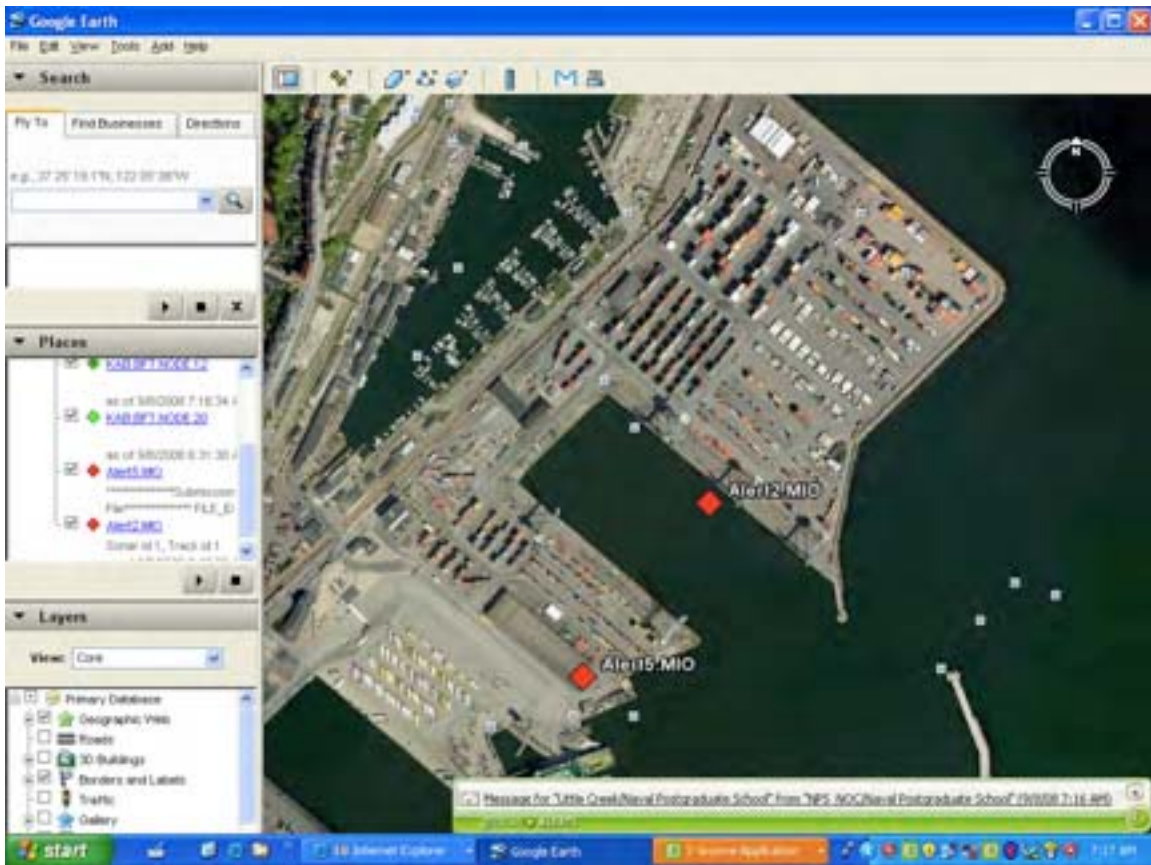


Figure 10 Sonar Alert biometrics from Demark seen in JSAS Situational Awareness Viewer Display screen

DNDO successfully retrieved the information that was sent by the boarding teams that were posted in JSAS. DNDO



could now make the determination of a positive or negative confirmation and post results in JSAS for boarding team to take action.

This experiment represents that interagency data sharing is instrumental in detecting and intercepting a possible terrorist attack on the United States. Interlinking data source that are currently in use have strong collaborative capabilities, however, when orchestrating such an event there are difficulties in establishing one-on-one communication because there were so many agencies involved they did not know if the messages posted within JSAS were directed to them for acknowledgement.

For example, DNDO received a readable spectrum analysis from the JSAS portal. It was not clear whether DNDO (in support of state and local agencies) should process the request analysis or LSS (in support of the DHS agencies). DNDO requested more information from the reporting agency through the JSAS portal because the spectrum information was incomplete (background readings, distance, location, etc.) There were no responses to messages in the JSAS portal and no means to confirm that the correct users ever received the request. In the end, the US Coast Guard also collected the spectrum from the JSAS portal and coordinated with LSS to conduct the analysis and adjudication of the spectrum. DNDO only became aware of this manifestation after LSS informed DNDO of the results. The DNDO watch officer needs more information and has instructed the sender to call him. There is no confirmation that his request has been received.

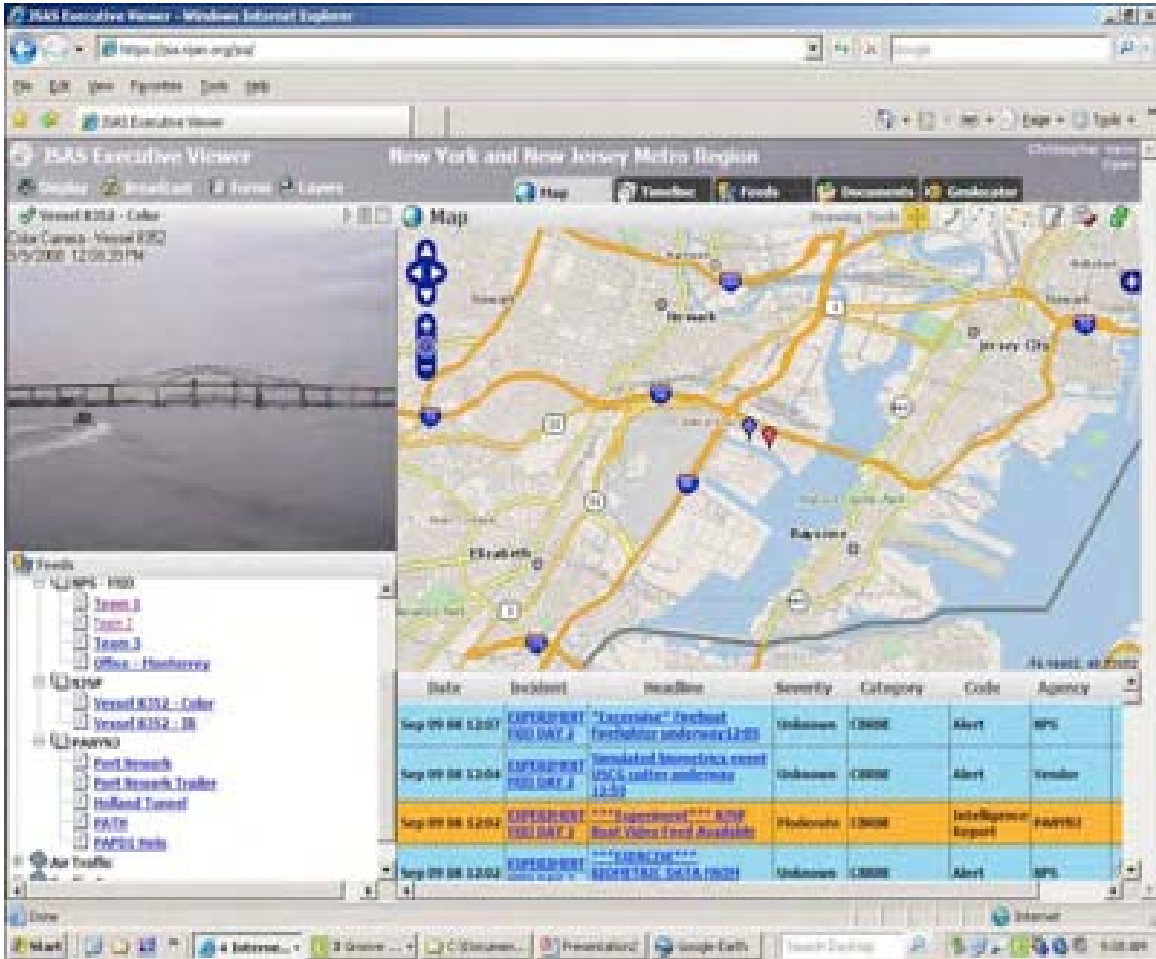


Figure 11 Streaming video frame (upper left corner) from NJSP vessel conducting search for small target vessels in Newark, NJ Harbor MIO

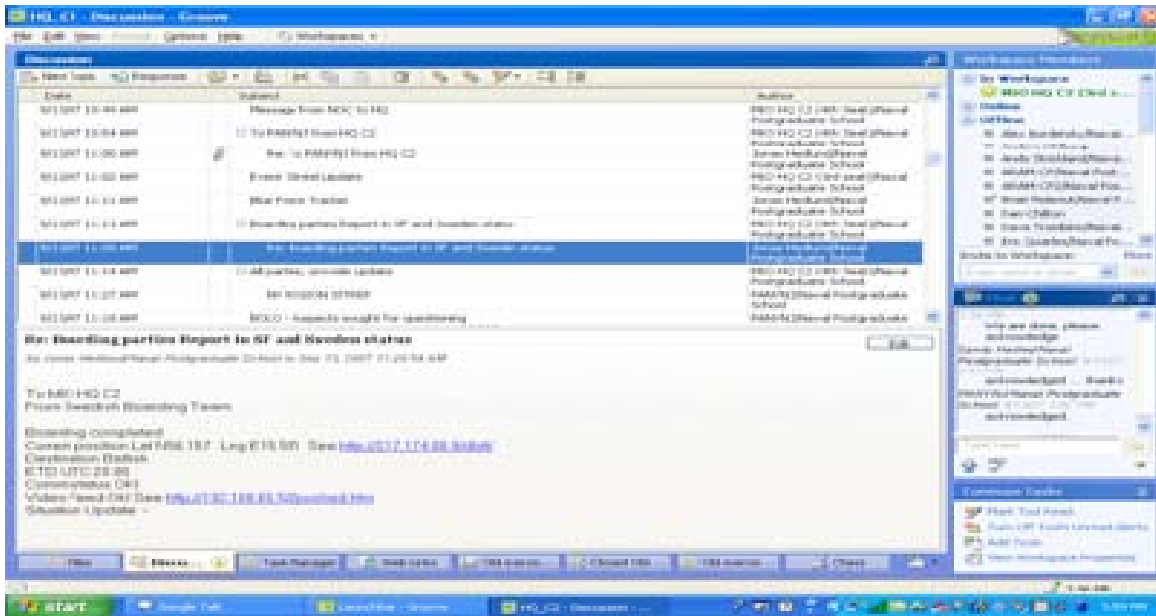


Figure 12 Small craft interdiction Groove Workspace MIO 07-04

***DNDO DATA SHARING RECOMMENDATIONS:***

The JSAS portal should have two features added to prevent the confusion. The first feature should include 1) a requester entry, 2) intended audience and 3) action requested. For examples; From PANYNJ to DNDO, Request analysis of Spectrum located at. The second feature should be 1) a confirmation of acceptance from the intended audience and 2) a comment block. For example: DNDO has received the information request and cannot accurately process until the following information is received. These features would allow for positive communication between the requester and intended audience, while providing situational awareness to all participants.

The following are the actual logged events that depict how information was being exchanged between agencies using different collaborative tools.

0808: NPS NOC online—Groove Chat

0924: NOC transfers JSAS C2, lost connectivity due to weather—Groove Chat

1158: Port Newark patrol underway—Groove Chat

1204: Coast Guard cutter underway—JSAS  
For Official Use Only 33 / 80

1205: New York fire boat underway—Groove Chat

1207: New York fireboat underway—JSAS

1216: New Jersey state police passed the target vessel at 100 meters, no source detected—JSAS

1218: New Jersey state police detected source at 51 feet off target vessel stern—JSAS

1220: Coast Guard cutter detects biometrics vessel at 40.42.206-74, .07.061 - JSAS

1222: Coast Guard Cutter makes contact with subject vessel—Groove Chat

1222: New Jersey State Police detects vessel to align starboard side with the stern of target vessel. Detected source at 10 meters—JSAS

1227: New Jersey State Police passed target vessel approximately 4 meters at 14 knots. Detection level 361 gamma counts.—JSAS

1227: Coast Guard cutter contacts confirmation at 40.42.206N 074.07.061W at 12:18 ARAM  
Radiation Monitor identified Cesium 137- JSAS

1314: New York fireboat has detected 18 micros from target vessel in position 40.41.928N 074-05.827W - JSAS

1318: New York harbor vessel has target vessel in sight—Groove Chat

1318: New York fireboat detects biometrics data

indicates high risk individual on target vessel  
Bobby Al-sir-bg, suspect has been detained and  
waiting for instructions - JSAS

1320: New York fireboat approaching target  
vessel-Groove Chat

1320: New York State Police gamma event 17  
distance 72\ Speed 5 Knot ID. Cs137

1321: New York fireboat has detected 18 micros  
from target vessel-Groove Chat

1329: Jersey City fireboat Gama Source detection  
lat: 40.42.35N and Long:0.74.07.11W: Two  
mrams by thermo, 38 mrams by identifier, 9.5  
mrams by thermo fisher FH671-Groove Chat

1333: Index all vessels returning to port-Groove  
Chat

1334: UCC reporting index-Groove Chat

1339: Exercise concludes - JSAS

Concluding the experiment there was an informal hot  
wash among all the participants discussing and highlighting  
items they thought were items to be improved in the next  
MIO. Below are a few issues and recommendations that were  
brought forth by the DNDO.

**Issue:** no intuitive method to conduct persist  
informal discussions.

**Discussion:** Many collaborative tools have a chat  
feature that encourages informal, multi-user  
discussions. Chat discussions are where much of  
the information is shared between subject matter  
experts, decision makers, action officers, and

first responders. The informal attribute allow for intelligent people to ask questions on subjects that they are not necessarily experts on (no stupid question concept) and get a more than one explanation. The consumer can then decide when they have enough information and bad information can be refuted by the community in near real time. This can be equated to the "hallway conference" or conversations that occur at the "coffee pot or drinking fountain." For instance, Participant 1 reports the location of a vehicle at coordinates X, Y. A first responder or command center can reply to the thread indicating that those coordinates were as of 2 hours ago, the new location as of this time are coordinate X1, Y1.

**Recommendation:** Create a persistent discussion thread that facilitates the informal discussion that can aid in situational awareness. This is not intended to replace the formal alerts or instant message-point-to-point communications.

**Issue:** Key for Alerts is not intuitive

**Discussion:** The alerts in JSAS have several color codes (Green, Yellow, Blue, Orange, and Red) and statuses (unknown, none, minor, moderate, severe, extreme) that do not map to the actual event description. For instance a video feed was reported as both Orange/Moderate and Green/None. This is just one example of several inconsistencies.

**Recommendation:** Have a legend or key on the alert section that can be hidden or minimized once it is learned. Also, have an active adjudicator who can adjust the status of the alert and add a note as to why the change occurred.

**Issue:** Naming convention

**Discussion:** The naming convention for Alerts and Files do not inform the users as to the content of the alerts or files. In the alerts, some entries were listed as Jersey City Marine 1, but the actual message was Thermo Fisher-Identifier-38 yRem Hr . . . Their title did not inform the user as to the contents of the message. Also, when files are downloaded, they are given a generic name starting with F followed by numbers.

**Recommendation:** Create and enforce a naming convention. Have an active adjudicator who can adjust the status of the alert AND add a note as to why the change occurred.

**Issue:** NPS's Observer Notepad refresh feature deletes comments

**Discussion:** When entering text into the system and the system automatically refreshes, all unsubmitted text is erased.

**Recommendation:** Have the refresh feature only update submissions without deleting text that is currently in the dialogue box.

**Notes:** Spectrum received by DNDO watch officer. File is readable with the specific software. The DNDO watch officer needs more information and has instructed the sender to call him. There is no confirmation that his request has been received. (Bordetsky 2008)

In the above experiment there were several collaborative tools used to identify, detect and intercept the target vessel. The three main collaborative tools were JSAS, GROOVE and NPS Situational Awareness (SA) which all have their distinct capabilities. NPS SA is primarily a common operating picture (COP) tool, GROOVE is primarily a collaborative tool to share thoughts, documents and video with other participants while JSAS is a hybrid of both the common operating picture and the collaborative tool. These tools were used successfully by passing information between them using MITRE'S cursor on target (CoT), which is a machine-to-machine language designed to communicate quickly and accurately. These collaborative tools all have the ability to speak the language of CoT, which allowed the interoperability of information to flow between data sources. As noted from the above difficulties sharing within JSAS became troublesome on the first day of the experiment due to several undefined issues possibly relating from user experience and connectivity. On the second day of the experiment the boarding teams focused their efforts on sharing data within GROOVE, which proved to be a strong



source for collaborative efforts. JSAS is an outstanding tool for collaborating however there are issues that may relate to the robustness as stated in the above issues.

The Naval Postgraduate School is continuing the experiment with MIO and will be improving on every situation, such as the scenario above. This experiment is not a substitute for solving the larger problems within DHS and around the government, but is an example of what is possible of the machine-to-machine language designed of CoT, and if further research is conducted the need for interoperability will be achieved. DHS uses a process called CAP (Common Alert Protocol), which is an XML-based data format for exchanging public warnings. The possibilities of both language designs will future our nation in achieving interoperability. For future research, I offer the following hypothesis: If agencies are collaborating in a dynamic data-sharing environment, then there should be a mechanism to conduct one-on-one side bar conversations, file sharing, shared picture analysis and instant messaging.

## VI. CONCLUSION

### A. UNITY—SHARING THE SECRET

The focus of this thesis was to discuss and educate the reader with the importance of interoperability between agencies and highlight where we are in the process. The focus is on how the Department of Homeland Security is having difficulties developing an effective solution solving the ability to share information horizontally and vertically between agencies. Several other federal, state, and local agencies across the entire United States are having the same difficulties. Taxpayers are paying billions of dollars a year for the development of software that is not fulfilling the needs to share information between agencies. For example, the Department of Homeland Security's HSIN is not providing the level of information needed by its users so they are redeveloping NextGen HSIN for sixty-two million dollars. Why are they redeveloping a network that does not address the users requirements and then name it NextGen HSIN? Maybe this is going to be another sixty-two million-dollar mistake to the taxpayers. The Government Accountability Office (GAO) and the Office of the Inspector General (OIG) are agencies that follow, evaluate and provide oversight of acquisition development throughout the government. You can "Google" these reports and many of them are very detailed and provide strong suggestions on how to proceed in indentifying ways to fix shortcomings. However many of these reports fall on deaf ears and problems that could have been resolved proceed with development while costing the taxpayer billions that could have been avoided

if only someone was listening. Agencies that are developing substandard software are not being held accountable for wasting taxpayer's monies and most importantly the safety of the United States for not enabling a fully functional information-sharing framework.

The information sharing networks that are being developed throughout the federal, state, and local government focus on compartmentalization of information such as Department of Homeland Security's HSIN where Community of Interest are the key ways to share information with other agencies with the same law enforcement mission. However, there could be vital information in another COI but someone has to ask for that information. No one will ask for the information because they do not even know that information exists, or someone asks but the information cannot be shared because of the current rules protecting information. What this represents is that we are still operating in a "need to know" era before we can share.

With the current rules governing over sharing information, agencies still encourage over classification of material and compartmentalization of information between agencies. We are still rewarding the ability to protect information instead of trying to share. We are continuing to follow our past of a "need to know" and not really grasping the concept of the "need to share" mental thought. We have the technological advances to enable agencies to develop suitable information sharing platforms. Even though we have policies helping to jump-start and streamline the idea of sharing information to protect and defend our nation, we still do not have strong rules for acquiring,

accessing and sharing and using vast stores of public and private data that may be available. (The 9-11 Commission Final Report) Without the rules and laws that will protect the ability to share information, agencies will continue to protect their information because there is no repercussion for protecting.

Any software that is being developed must take the stakeholder requirements to heart when in development. Requirements are the basis for identifying what is really needed by stakeholders to enable a network to be successful. This is one of the most common mistakes when in development, not getting quality requirements from your user.

The overall success of developing a successful interagency information-sharing framework is important in numerous areas of protecting and defending our nation. In this thesis, the author endeavored to tie together information sharing and Maritime Port Security and how the two interrelate. The Maritime Ports of the United States are vulnerable to attack and sharing information throughout the federal, state and local government will increase our chances for detecting a possible attack and defeating our adversaries in protecting our nation. Maritime Port Security is just one area that will benefit from working together and sharing information. Law enforcement across the spectrum will capitalize on the investment to share information.

In conclusions and suggestions to further develop information sharing and protecting our nation the following is proposed:

1. Provide rules and polices needed to foster and reward sharing of information.
2. Provide decision makers with knowledge that will change mental thought and promote sharing among between agencies.
3. Before developing a software project fully understand the requirements and quality attributes from your stakeholders. Once you have them they need to be implemented in an incremental fashion during development.
4. Implement a decentralized network model: this is where agencies still have their own databases, but these databases could be searched by other agencies through designed agency lines. Information is protected through "setting privileges" approach that will control access to data by not allowing full access to the entire network. This replaces the current structure of a hub and spoke idea where all data is located in one central location, which contributes to a single point of failure. (Markle Foundation 2003)

To be successful in implementing the above-proposed suggestions in strengthening our nation the government requires strong leadership. There are a series of issues that need to be address before we are able to share information seamlessly across the federal government. I believe it starts with the commander in chief to enhance incentives to share information. People in general need some sort of incentive to come to a realization that interoperability is a vital concept that needs to be

implemented. Without incentives its still easier and safer to safe guard your information. "Why go out of my way and share if nothing is in it for me?" some people may ask themselves.

I also believe there is a classification issue that still exists between agencies. DHS encompasses many agencies and there are still trust issues. Just because DHS now encompasses several disparate agencies does not eliminate the trust element among agencies.

You can have all the facts and figures, all the supporting evidence, all the endorsement that you want, but if you don't command trust, you won't get anywhere. *Nail Fitzgerald* (Covey 2006)

Technique and technology are important, but adding trust is the issue of the decade. *Tom Peters* (Covey 2006)

When you connect database through middleware there has to be permissions granted by some authority. As mentioned above the concept of a decentralized network is the key concept to connecting existing databases. However, I would recommend that a centralized access list be maintained by DHS to grant permissions on viewing/access capabilities. This allows one hierarchical entity to oversee who is on the network and monitor the areas that need to be highly protected from potential insider and outsider attacks.



Figure 13 A Coast Guard RHIB off Manhattan on the morning of 11 September 2001 by Chan Irwin.

## LIST OF REFERENCES

- Bordetsky, Alex. 2008. CENETIX. After Action Report, TNT 08-4 MIO Experiment, (September 8-12).
- Covey, Stephen M. R. 2006. The Speed of Trust: The One Thing that Changes Everything. October. Simon and Schuster.
- Deffer, Frank W. Department Of Homeland Security. 2006. Statement of Frank W. Deffer, Assistant Inspector General, Information Technology U.S. Department of Homeland Security Before the Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. U. S. House of Representative.
- Department of Homeland Security. Department of Homeland Security Components  
<http://www.dhs.gov/xabout/structure/>. (accessed January 12, 2009).
- Department of Homeland Security. Figure of Department of Homeland Security Agencies.  
[http://www.dhs.gov/xabout/structure/editorial\\_0644.shtm](http://www.dhs.gov/xabout/structure/editorial_0644.shtm)  
. (accessed January 28, 2009).
- Department of Homeland Security. 2008. Department Homeland Security Role in State and local Fusion Centers is Evolving. Homeland Security Fusion Center Locations. Office of Inspector General. OIG-09-12.
- Department of Homeland Security. 2006. Homeland Security Information Network Could Support Information Sharing More Effectively. Diagram of Communities of Interests, Office of Inspector General; Homeland Security Information Network. OIG-06-38.
- Department of Homeland Security. Homeland Security Information Network  
[http://www.dhs.gov/xinfoshare/programs/gc\\_1156888108137.shtm](http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm) (accessed January 14, 2009).



Department of Homeland Security. Log on Screen into HSIN, <https://auth.hsin.gov/auth/UI/Login?service=ADAuth2&goto=https%3A%2F%2Fcs.hsin.gov%3A443%2F> (accessed on February 2, 2009).

Department of Homeland Security. 2008. Office of Inspector General. DHS's Efforts to Improve Homeland Security Information Network. OIG-09-07.

Department of Homeland Security. 2007. Operations Directorate National Operations Center. Privacy Impact Assessment. [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_ops\\_hsin.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_hsin.pdf) (accessed on January 20, 2009).

Department of Homeland Security. United States Customs and Border Protection. <http://www.cbp.gov/> (accessed on October 15, 2008).

Department of Homeland Security. United States Coast Guard. U.S. Coast Guard Missions. <http://www.uscg.mil/top/missions/> (accessed on October 15, 2008).

Endsley, Mica R., Charness Neil, Ericsson Anders K., Feltovich Paul J., Hoffman Robert R., 2000. Situation Awareness Analysis and Measurement. Cambridge University Press. New York.

Endsley, Mica R., Charness Neil, Ericsson Anders K., Feltovich Paul J., Hoffman Robert R., 2006. Situation Awareness Analysis and Measurement. Diagram of The Information Gap: Theoretical Underpinnings of Situation Awareness. Cambridge University Press. New York.

Eshel, David. 2005. Maritime and Port Security white Paper, The Threat of Maritime Terrorist: Defense Update. Duos Technologies, Inc., Jacksonville, FL.

Frittelli, John F. 2005. CRS Report for Congress, Port and Maritime Security: Background and Issues for Congress, updated May 10, 2005.

Goslin, Charles. 2008. Maritime and Port Security White Paper. Duos Technologies, Inc., Jacksonville, FL.

- Harris, William. 2007. Homeland Security Information Network: "Moving Past the Missteps Toward Better Information Sharing."  
[www.homeland.house.gov/SiteDocuments/20070510132121-04354.pdf](http://www.homeland.house.gov/SiteDocuments/20070510132121-04354.pdf) (accessed on December 5, 2008).
- Holmes, Allan. 2009. Technology and the Business of Government; Information Sharing.  
[http://www.nextgov.com/the\\_basics/tb\\_20090130\\_5740.php](http://www.nextgov.com/the_basics/tb_20090130_5740.php) (accessed on February 23, 2009).
- Information Sharing Environment, Background & Authorities.  
<http://www.ise.gov/pages/background.html>. (accessed November 6, 2008).
- International Atomic Energy Agency. Illicit Nuclear Trafficking Statistics: January 1993 - December 2004.  
[http://www.iaea.org/NewsCenter/Features/RadSources/Fact\\_Figures2004.html](http://www.iaea.org/NewsCenter/Features/RadSources/Fact_Figures2004.html) (accessed on January 23, 2009).
- Irwin Chan. 2001. Photo of a Coast Guard RHIB off Manhattan on the morning of 11 September 2001. Photo was taken by Chan Irwin and was provided courtesy of Mike Harmon  
[http://www.uscg.mil/history/WEBORALHISTORY/911\\_Photo\\_Index.asp](http://www.uscg.mil/history/WEBORALHISTORY/911_Photo_Index.asp) (accessed on March 5, 2009).
- Letter from Homeland Security Committee to the Acting Deputy of Homeland Security,  
<http://homeland.house.gov/SiteDocuments/20080118152930-40065.pdf> (accessed on February 2, 2009).
- Markle Foundation. 2003 Creating a Trusted Information Network for Homeland Security.  
[www.markle.org/downloadable\\_assets/nstf\\_report2\\_full\\_report.pdf](http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf) (accessed February 28, 2009).
- Moncel, Remi. 2009. World resources institute. President Obama's Open Government: Welcome First Steps.  
<http://www.wri.org/stories/2009/01/president-obamas-open-government-welcome-first-steps>. (accessed on February 23, 2009).
- National Commission on Terrorist Attacks Upon the United States. 9-11 Commission Report. [www.9-11commission.gov/report/911Report.pdf](http://www.9-11commission.gov/report/911Report.pdf) (accessed on February 25, 2009).

National Nuclear Security Administration. Report on Mega-ports Initiative from the National Nuclear Security Administration.  
[http://nnsa.energy.gov/nuclear\\_nonproliferation/1641.htm](http://nnsa.energy.gov/nuclear_nonproliferation/1641.htm) (accessed on 23 January 2009).

Office of Director of National Security. 2008. United States Intelligence Community Information Sharing Strategy. New Information Sharing Diagram.  
[www.dni.gov/reports/IC\\_Information\\_Sharing\\_Strategy.pdf](http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf) (accessed February 23, 2009).

Pellicci, Jack. Security International; Overcoming Obstacles to a security Common Operational Picture.  
<http://www.security-int.com/categories/security-common-operational-picture/overcoming-obstacles-to-a-security-common-operational-picture.asp> (accessed on February 19, 2009).

Stone, Eric. 2007. Meanderings. Ships and Other Big things at Sea. Example of container ship entering U.S. port,  
<http://www.ericstone.com/2007/09/ships-and-other-big-things-at-sea.html> (accessed on February 2, 2009).

The National Archives. Presidential Executive Order 13356; Strengthening the Sharing of Terrorism Information To Protect Americans <http://www.archives.gov/federal-register/executive-orders/2004.html> (accessed on November 2, 2008).

Tyler, Patrick E. 2002. Maritime and Port Security white Paper, Duos Technologies, Inc., Jacksonville, FL.

United Nations. 2002. United Nations Conference on Trade and Development, Review of Maritime Transport. Report presented by the UNCTAD in New York and Geneva.

United States Government. Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.  
[www.intelligence.senate.gov/laws/pl108-458.pdf](http://www.intelligence.senate.gov/laws/pl108-458.pdf) (accessed October 1, 2008).

United States Government Accountability Office. 2007. GAO, Maritime Security; One Year Later: A progress report on the SAFE Port Act. October.

Wagner, Breanne. 2007. National Defense Industrial Association (NDIA) Business and Technology Magazine. Reluctance to Share Information Hampers Counterterrorism Efforts. September. <http://www.nationaldefensemagazine.org/archive/2007/September/Pages/Reluctance2513.aspx> (accessed November 11, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX: SUPPORTING INTEROPERABILITY

### A. PRESIDENTIAL EXECUTIVE ORDER 13356

"By the authority vested in me as President by the Constitution and laws of the United States of America, and in order to further strengthen the effective conduct of United States intelligence activities and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby ordered as follows:

Section 1. Policy. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:

(a) Give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; and

(b) Protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities."

**B. LETTER FROM HOMELAND SECURITY COMMITTEE**

**BENNIE G. THOMPSON, MISSISSIPPI**  
CHAIRMAN



**PETER T. KING, NEW YORK**  
RANKING MEMBER

**One Hundred Tenth Congress**  
**U.S. House of Representatives**  
**Committee on Homeland Security**  
**Washington, DC 20515**  
January 17, 2008

The Honorable Paul A. Schneider  
Acting Deputy Secretary  
Department of Homeland Security  
Washington, D.C. 20528

Dear Mr. Schneider:

For the past several years, the Committee on Homeland Security has been closely monitoring the development of the Homeland Security Information Network (HSIN), the Department of Homeland Security's primary means for communicating sensitive but unclassified information (SBU) to its partners in the law enforcement, emergency responder, and private sector communities. On October 26, 2007, Committee staff met with Mr. Wayne Parent, the Deputy Director of the Office of Operations Coordination, and Ms. Theresa Phillips, the HSIN Program Manager, to discuss the current status of the HSIN and ongoing efforts to make it interoperable with other information sharing systems already in use by State, local, and tribal law enforcement and other entities. Both Mr. Parent and Ms. Phillips reported significant progress since our May 10, 2007 intelligence subcommittee hearing titled, "Fixing the Homeland Security Information Network: Finding the Way Forward For Better Information Sharing". Their update to staff was very welcome news about a program with ongoing challenges.

We recently learned, however, that on October 27, 2007 – one day after the staff briefing with Mr. Parent and Ms. Phillips – you issued a Memorandum that announced that the HSIN would be replaced. Specifically, your Memorandum describes a new "DHS Portal Consolidation Program" that will result in an "innovative, federally compliant [portal] environment that will replace the current HSIN platform and facilitate secure access to DHS information and services for all user communities . . ." Toward that end, your Memorandum (1) directed all Department components to stop any new development and enhancements to existing portal environments on the HSIN; (2) required the HSIN Program Management Office to deliver a requirements document for the collaboration and SBU portal within thirty days and [to] provide an acquisition plan within sixty days; and (3) mandated that all DHS components submit their operational data, service and technical portal architectures, including requirements, to the Chief Information Officer. You concluded your Memorandum by stating that, "DHS will realize substantial monetary savings and enhanced mission performance, with measurable results being achieved early in the transition. DHS will increase its information sharing

capabilities, and improve user satisfaction by providing the stakeholders, DHS employees and citizens with a collaborative, innovative and scaleable web communications tool.”

While we agree that taking the troubled HSIN program in a new direction may make sense, we are surprised that your plan was not briefed to Committee staff on October 26 or brought to our attention subsequently. It is unacceptable that the Department would brief the Congress on the status of the program on one day and dramatically alter that program the next. We accordingly require responses to the following questions:

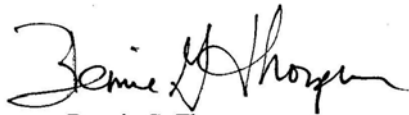
- During the implementation of the DHS Portal Consolidation Program, what will happen to the existing HSIN? Will it continue to be used by all stakeholders during the changeover to the new enterprise SBU portal? If so, how and with what limitations? Most importantly, will any of the HSIN development effort to date be reused with the new enterprise SBU portal, or has the entire HSIN effort until this point been wasted?
- How much money has been spent on the HSIN to date – including the development of the portions of it that will now be replaced under the new DHS Portal Consolidation Plan – and who have the private sector contractors been for each stage of the HSIN? What specific work has each contractor been responsible for, and whose work is now being overridden by the new DHS Portal Consolidation Plan? Who will be tapped in the contractor community to implement the HSIN’s new direction and at what estimated cost?
- HSIN’s program management has historically been very weak. What changes are being made to improve the program management of the new enterprise SBU portal? What process will be used to validate the new enterprise SBU portal with appropriate user communities, and what steps have been taken in that regard?
- What is planned for States that use HSIN as their primary information sharing system? Were States consulted about the changes you are now making, and if so, how is their input being incorporated?
- Congress and many in the State and local law enforcement communities have been pushing for better HSIN integration with current systems such as Law Enforcement Online (LEO), the Law Enforcement Information Exchange (LINX), and the Regional Information Sharing System (RISS). To what extent will the new HSIN integrate with these systems?
- On what do you base your statement that “DHS will realize substantial monetary savings” with the new enterprise SBU portal? What analysis have you done that has resulted in your conclusion and who conducted that analysis for the Department? Moreover, how will the cost savings that you describe be realized and how much money will be saved as a result of the changeover to the new enterprise SBU portal?



- You note that the current HSIN site looks “governmental” as if that is a bad thing. What does the “governmental” appearance of the HSIN network have to do with its usefulness? Is the HSIN being revamped merely to make it look less “governmental”?
- To what extent have you consulted the Program Manager of the Information Sharing Environment in the Office of the Director of National Intelligence when determining that such a dramatic overhaul of the HSIN was necessary?

Please provide written responses to these questions by February 14, 2008, along with any written version of the DHS Portal Consolidation Program, material provided to you by the HSIN Program Management Office in response to your Memorandum, and the contracts for the HSIN that DHS has been party to since the HSIN’s inception. If you have any questions, please contact Cherri Branson or Tom Finan with the Committee’s Majority staff at 202-226-2616 or Joe Vealencis with the Committee’s Republican staff at 202-226-8417. We look forward to hearing from you.

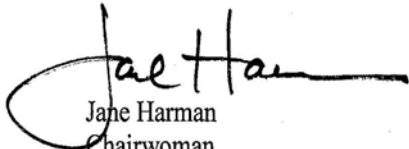
Sincerely, \_\_\_\_\_



Bennie G. Thompson  
Chairman  
Committee on Homeland Security



Peter T. King  
Ranking Member  
Committee on Homeland Security



Jane Harman  
Chairwoman  
Subcommittee on Intelligence,  
Information Sharing, and Terrorism  
Risk Assessment  
Committee on Homeland Security



David Reichert  
Ranking Member  
Subcommittee on Intelligence,  
Information Sharing, and Terrorism  
Risk Assessment  
Committee on Homeland Security

BGT/uf

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Fort Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California